H-995

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

S. SAWADA et al

Serial No. 09/893,004

Filed: June 28, 2001

ATTN: Manager,
Applications Branch

For: COMMUNICATION APPARATUS FOR ROUTING OR DISCARDING A PACKET SENT FROM A USER TERMINAL

TRANSMITTAL OF LATE DECLARATION AND CERTIFIED PRIORITY DOCUMENT

Commissioner for Patents
Washington, D.C. 20231

September 20, 2001

Sir:

Responsive to the NOTICE TO FILE MISSING PARTS OF APPLICATION - FILING DATE GRANTED mailed August 21, 2001, Applicants submit herewith the executed Declaration and Power of Attorney, along with the required surcharge as set forth in 37 CFR 1.16(e).

Our check in the amount of $130.00 is attached.

As required, a copy of the NOTICE (PART 2) of August 21, 2001 is enclosed herewith.

Also submitted is a certified priority document of corresponding Japanese Patent Application No. 2000-195706 filed June 29, 2000 for the purpose of claiming foreign priority under 35 U.S.C. § 119. An indication that this document has been safely received would be appreciated.

Please charge any additional fees which may be required, or credit any overpayment to our Deposit Account No. 50-1417.

Respectfully submitted,

Daniel J. Stanger
Registration No. 32,846
Attorney for Applicant(s)

MATTINGLY, STANGER & MALUR
1800 Diagonal Rd., Suite 370
Alexandria, Virginia 22314
(703) 684-1120
Date: September 20, 2001

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年　６月２９日

出願番号
Application Number: 特願２０００－１９５７０６

出願人
Applicant(s): 株式会社日立製作所

２００１年　４月２０日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３０３２４２８

【書類名】　特許願
【整理番号】　P0264JP
【提出日】　平成12年 6月29日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 29/02
【発明者】
【住所又は居所】　神奈川県秦野市堀山下１番地　株式会社日立製作所　エンタープライズサーバ事業部内
【氏名】　澤田　素直
【発明者】
【住所又は居所】　神奈川県秦野市堀山下１番地　株式会社日立製作所　エンタープライズサーバ事業部内
【氏名】　綿貫　達哉
【発明者】
【住所又は居所】　神奈川県秦野市堀山下１番地　株式会社日立製作所　エンタープライズサーバ事業部内
【氏名】　野崎　信司
【特許出願人】
【識別番号】　000005108
【氏名又は名称】　株式会社日立製作所
【代理人】
【識別番号】　100107010
【弁理士】
【氏名又は名称】　橋爪　健
【手数料の表示】
【予納台帳番号】　054885
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ネットワーク間接続装置及びネットワークシステム

【特許請求の範囲】

【請求項１】

ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるネットワーク間接続装置であって、

複数のネットワークインターフェースと、

パケットを送信すべき前記ネットワークインターフェースを特定するための情報を含むアドレス学習テーブルと、

前記学習テーブルを参照して、前記ネットワークインターフェースの状態に基づいて、パケットの中継先を選択すると共に、ユーザ端末、認証サーバ及びファイルサーバ間のパケットを中継又は廃棄するパケット中継部と、

特定のネットワークインターフェースの状態を接続状態、非接続状態及び状態なしのいずれかの状態に変更する指示を保持する状態変更指示パケットを、前記パケット中継部を介して認証サーバから受信する状態変更指示パケット処理部と、

特定のネットワークインターフェース内にそれぞれ設けられ、前記状態変更指示パケット処理部からの状態変更指示パケットを受信すると共に、該状態変更指示パケットに基づいて、特定のネットワークインターフェースの状態を接続状態、非接続状態及び状態なしのいずれかの状態に変更する状態管理部と

を備えたネットワーク間接続装置。

【請求項２】

前記ネットワークシステムでは、ネットワーク及びルータを介して配されたユーザ端末に動的にアドレスを配布するアドレス割り当てサーバをさらに備え、

受信したパケットの送信元アドレスを登録するフィルタリングテーブルをさらに備え、

前記状態変更指示パケット処理部は、

前記フィルタリングテーブルに登録された特定のアドレスを、前記アドレス学

習テーブルに登録するように指示する状態変更指示パケットを受信した場合、該特定のアドレスをアドレス学習テーブルに登録し、

パケットの宛先アドレスが、アドレス学習テーブルに登録されている場合、パケットを中継し、

パケットの宛先アドレスが、アドレス学習テーブルに未登録であり、かつ、前記フィルタリングテーブルに登録され、パケットの送信元アドレスが、ルータ又は認証サーバである場合、パケットを中継するようにした請求項１に記載のネットワーク間接続装置。

【請求項３】

前記ネットワークインターフェースは、ネットワークが使用可能であるかどうかを検出する回線断検出部をさらに備え、

前記状態管理部は、

前記回線断検出部により回線断が検出された場合、回線断が検出されたネットワークインターフェースの状態を非接続状態に変更し、

前記認証サーバによりユーザ端末が認証を受けた場合、該ユーザ端末に接続されたネットワークインターフェースの状態を接続状態に変更し、

前記パケット中継部は、

非接続状態のネットワークインターフェースからパケットを受信した場合、パケットを、非接続状態又は接続状態のネットワークインターフェースには中継せず、特定のネットワークインターフェースにのみ中継し、

接続状態のネットワークインターフェースからパケットを受信した場合、パケットを、非接続状態のネットワークインターフェースには中継しないようにした請求項１又は２に記載のネットワーク間接続装置。

【請求項４】

ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるネットワーク間接続装置であって、

ネットワークに接続するための物理インターフェースと、

パケットの中継先を選択するパケット中継部と、

パケットを中継又は廃棄するための情報を含むフィルタリングテーブルと、前記フィルタリングテーブルの内容に基づいて、パケットを廃棄又は前記パケット中継部に送信するパケット処理部とを有し、前記物理インターフェースとパケット中継部との間に配され、パケットフィルタリングを行うフィルタリング処理部と、

前記フィルタリング処理部に対して、前記認証サーバからのフィルタリング変更指示を送信し、かつ、受信したパケットを全て廃棄するように初期設定された前記フィルタリングテーブル内の情報を、前記認証サーバからの指示に基づいて変更し、前記認証サーバにより認証を受けたユーザ端末のアドレスを送信元アドレスとするパケットを前記ファイルサーバに中継するための情報を、前記フィルタリングテーブルに順次追加するフィルタリング変更指示処理部と

を備えたネットワーク間接続装置。

【請求項５】

ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるネットワーク間接続装置であって、

ユーザ端末、認証サーバ及びファイルサーバからのパケットを送受信するネットワークインターフェースと、

認証サーバにより認証を受けたユーザ端末のアドレスを登録するＩＰアドレス登録表と、

前記ＩＰアドレス登録表に登録されたアドレスを送信元アドレスとするパケットを中継し、ＩＰアドレス登録表に未登録のアドレスを送信元アドレスとするパケットはカプセル化した後、特定のアドレス宛に送信するパケット中継部と

を備えたネットワーク間接続装置。

【請求項６】

請求項１乃至５のいずれかに記載のネットワーク間接続装置と、

前記ネットワーク間接続装置にネットワークを介して接続されたユーザ端末と、

ファイルサーバと、

前記ユーザ端末に対して、前記ファイルサーバへのアクセスを許可するための認証を行う認証サーバと
を備えたネットワークシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワーク間接続装置及びネットワークシステムに係り、特に、ＬＡＮスイッチやルータ等を用いたネットワークの不正使用を防止するネットワーク間接続装置及びネットワークシステムに関する。

【０００２】

【従来の技術】

近年、各種ネットワークが保持する情報に対する信用を確保するために、ネットワークの利用を制限する情報セキュリティ技術の必要性が認識されている。一方、ネットワークの利便性を考えて、例えば、ＩＥＥＥ（Institute of Electrical and Electronics Engineers, Inc.）で規定されているＣＳＭＡ／ＣＤ（Carrier Sense Multiple Access with Collision Detection）型の８０２．３ネットワークに代表されるＬＡＮ（Local Area Network）では、ネットワークに端末を接続しさえすれば使用できるようになっている。

【０００３】

また、ＩＥＴＦ（Internet Engineering Task Force）で標準化されたＤＨＣＰ（Dynamic Host Configuration Protocol）を用いれば、新たに接続された端末に対して自動的にアドレスを割り当てることができる。これらのネットワークとノート型パソコンのような可搬型の端末により、自由な場所で必要な時にネットワークを利用できる情報コンセントシステムが登場している（例えば、“生徒のための、生徒による、生徒のネットワーク作り物語”，pp.66, UNIX USER, vol.8, No.4, APR.1 1999）。

【０００４】

【発明が解決しようとする課題】

しかしながら、ネットワークの利用が容易になることで、ネットワークの使用

許可を得ていない不正な利用者（不正ユーザ）であっても、ネットワークに端末を接続しさえすればネットワークを利用できてしまう場合が想定される。このため、ネットワークに接続されたファイルサーバなどの資源は、不正ユーザからの不正なアクセスにさらされるというセキュリティ上の不都合が生じてしまう。

【０００５】

こうした不正なアクセスの防止に用いられる技術として、ルータ等のネットワーク間接続装置によるパケットフィルタリングが知られている。しかし、パケットフィルタリングの条件は予め設定しておかなければならず、上述の情報コンセントシステムのように、任意の位置で動的に配布されたアドレスを用いているネットワークでは、予めパケットフィルタリングの条件を決めておくことは困難である。

【０００６】

本発明は、以上の点に鑑み、不正な利用者がネットワークを不正に利用することを防止するネットワーク間接続装置及びネットワークシステムを提供することを目的とする。

また、本発明は、ユーザが自由な位置で、その度に違うアドレスでネットワークに接続しても、そのユーザに対して許可されたネットワーク資源にしかアクセスできないネットワーク間接続装置及びネットワークシステムを提供することを目的とする。

【０００７】

【課題を解決するための手段】

本発明の第１の解決手段によると、

ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるネットワーク間接続装置であって、

複数のネットワークインターフェースと、

パケットを送信すべき前記ネットワークインターフェースを特定するための情報を含むアドレス学習テーブルと、

前記学習テーブルを参照して、前記ネットワークインターフェースの状態に基

づいて、パケットの中継先を選択すると共に、ユーザ端末、認証サーバ及びファイルサーバ間のパケットを中継又は廃棄するパケット中継部と、

特定のネットワークインターフェースの状態を接続状態、非接続状態及び状態なしのいずれかの状態に変更する指示を保持する状態変更指示パケットを、前記パケット中継部を介して認証サーバから受信する状態変更指示パケット処理部と、

特定のネットワークインターフェース内にそれぞれ設けられ、前記状態変更指示パケット処理部からの状態変更指示パケットを受信すると共に、該状態変更指示パケットに基づいて、特定のネットワークインターフェースの状態を接続状態、非接続状態及び状態なしのいずれかの状態に変更する状態管理部と

を備えたネットワーク間接続装置を提供する。

【０００８】

本発明の第２の解決手段によると、

ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるネットワーク間接続装置であって、

ネットワークに接続するための物理インターフェースと、

パケットの中継先を選択するパケット中継部と、

パケットを中継又は廃棄するための情報を含むフィルタリングテーブルと、前記フィルタリングテーブルの内容に基づいて、パケットを廃棄又は前記パケット中継部に送信するパケット処理部とを有し、前記物理インターフェースとパケット中継部との間に配され、パケットフィルタリングを行うフィルタリング処理部と、

前記フィルタリング処理部に対して、前記認証サーバからのフィルタリング変更指示を送信し、かつ、受信したパケットを全て廃棄するように初期設定された前記フィルタリングテーブル内の情報を、前記認証サーバからの指示に基づいて変更し、前記認証サーバにより認証を受けたユーザ端末のアドレスを送信元アドレスとするパケットを前記ファイルサーバに中継するための情報を、前記フィルタリングテーブルに順次追加するフィルタリング変更指示処理部と

を備えたネットワーク間接続装置を提供する。

【０００９】

本発明の第３の解決手段によると、

ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるネットワーク間接続装置であって、

ユーザ端末、認証サーバ及びファイルサーバからのパケットを送受信するネットワークインターフェースと、

認証サーバにより認証を受けたユーザ端末のアドレスを登録するＩＰアドレス登録表と、

前記ＩＰアドレス登録表に登録されたアドレスを送信元アドレスとするパケットを中継し、ＩＰアドレス登録表に未登録のアドレスを送信元アドレスとするパケットはカプセル化した後、特定のアドレス宛に送信するパケット中継部と

を備えたネットワーク間接続装置を提供する。

【００１０】

本発明の第４の解決手段によると、

上述に記載のネットワーク間接続装置と、

前記ネットワーク間接続装置にネットワークを介して接続されたユーザ端末と、

ファイルサーバと、

前記ユーザ端末に対して、前記ファイルサーバへのアクセスを許可するための認証を行う認証サーバと

を備えたネットワークシステムを提供する。

【００１１】

本発明の特徴のひとつとしては、複数のネットワークインターフェースとパケット中継手段とを有し、各ネットワークインターフェースが、接続状態、非接続状態、状態なしのいずれの状態であるかを保持する状態管理手段を有し、該各ネットワークインターフェースの状態が該パケット中継手段におけるパケットの中継先の選択に影響する。

【００１２】

本発明の他の特徴としては、状態変更指示パケット処理手段を有し、状態変更指示パケットで指示された前記ネットワークインターフェースの状態を該状態変更指示パケットで指示された状態に変更することができる。

【００１３】

本発明の他の特徴としては、前記各ネットワークインターフェースは回線断検出手段を有し、該回線断検出手段により回線断が検出されると該ネットワークインターフェースの状態を非接続状態に変更することができる。

【００１４】

本発明の他の特徴としては、初期化時に各ネットワークインターフェースの状態が非接続状態に初期化されるようにしてもよい。

【００１５】

本発明の他の特徴としては、非接続状態の該ネットワークインターフェースから受信したパケットを特定の該ネットワークインターフェースのみに中継することができる。

【００１６】

本発明の他の特徴としては、非接続状態の該ネットワークインターフェースから受信したパケットを、非接続状態あるいは接続状態の該ネットワークインターフェースに中継しないようにしてもよい。

【００１７】

本発明の他の特徴としては、接続状態の該ネットワークインターフェースから受信したパケットを非接続状態の該ネットワークインターフェースに中継しないようにしてもよい。

【００１８】

本発明の他の特徴としては、上述のネットワーク間接続装置を適用したネットワークシステムであって、認証を行ったユーザの使用する端末の接続されたネットワークインターフェースの状態を接続状態に変更するようにしてもよい。

【００１９】

本発明の他の特徴としては、上述のネットワーク間接続装置を適用したネット

ワークシステムであって、複数のネットワークインターフェース、パケット中継手段、フィルタリングテーブル、該フィルタリングテーブルの内容によってパケットフィルタリングを行うパケットフィルタリング手段、及び該フィルタリングテーブルの内容を外部からの指示により変更するフィルタリング変更指示処理手段を有し、初期状態では該フィルタリングテーブルの内容を全ての受信パケットを廃棄する用に設定されたネットワーク間接続装置に対し、外部からの指示で特定の送信元アドレスを持つパケットの中継を許可する内容を該フィルタリングテーブルに順次追加していくことができる。

【００２０】

本発明の他の特徴としては、上述のネットワーク間接続装置を適用したネットワークシステムであって、順次追加していく内容は、認証を受けたユーザが使用する端末のアドレスを送信元アドレスとして持つパケットの中継許可であるようにしてもよい。

【００２１】

本発明の他の特徴としては、複数のネットワークインターフェース、パケット中継手段、フィルタリングテーブル、アドレス学習テーブル及び状態変更指示パケット処理手段を有し、受信したパケットの送信元アドレスを該フィルタリングテーブルに登録し、該フィルタリングテーブル内に登録された特定のアドレスを該アドレス学習テーブルに登録するよう指示する状態変更指示パケットを受信した場合に、該状態変更指示パケット処理手段が該フィルタリングテーブルに登録された特定のアドレスを該アドレス学習テーブルに登録するようにしてもよい。

【００２２】

本発明の他の特徴としては、前記学習テーブルに登録されたアドレス宛のパケットを中継し、該学習テーブルに登録されてなく、かつ、前記フィルタリングテーブルに登録されているアドレス宛のパケットは、特定の送信元アドレスを有している場合にのみ中継することができる。

【００２３】

本発明の他の特徴としては、上述のネットワーク間接続装置を適用したネットワークシステムであって、認証を受けたユーザの使用する端末のアドレスを前記

学習テーブルに登録することを指示することができる。

【００２４】

本発明の他の特徴としては、複数のネットワークインターフェース、パケット中継手段、及びアドレス登録表を有し、該アドレス登録表に登録されたアドレスを送信元アドレスとするパケットは、中継し、該アドレス登録表に登録されていないアドレスを送信元アドレスとするパケットは、カプセル化した後、特定のアドレス宛に送信するようにしてもよい。

【００２５】

本発明の他の特徴としては、上述のネットワーク間接続装置を適用したネットワークシステムであって、前記アドレス登録表に登録されていないアドレスを送信元アドレスとするパケットをカプセル化して送信する特定のアドレスが、ユーザの認証を行う装置のアドレスであるようにしてもよい。

【００２６】

本発明の他の特徴としては、上述のネットワーク間接続装置を適用したネットワークシステムであって、認証を受けたユーザの使用する端末のアドレスを前記アドレス登録表に登録するようにしてもよい。

【００２７】

本発明の他の特徴としては、ネットワーク間接続装置の各ネットワークインターフェースで「非接続状態」かどうかを管理し、「非接続状態」である場合、通信を遮断するようにしてもよい。

【００２８】

本発明の他の特徴としては、ネットワークから端末が離脱した場合、この離脱を検出したネットワークインターフェースでは、自動的に「非接続状態」に切り替わるようにしてもよい。

【００２９】

本発明の他の特徴としては、ユーザに対して割り当てられたアドレスを把握し、この把握したアドレスに基づいてパケットフィルタリングの設定を行うようにしてもよい。

【００３０】

【発明の実施の形態】

以下、図面を用いて本発明の実施の形態を詳細に説明する。

（第1の実施の形態）

図１は、本発明に関するネットワーク間接続装置の第１の実施の形態の構成図である。

ＬＡＮスイッチ１００は、例えば、パケット中継手段１０１、複数のネットワークインターフェース１０２～１０７、アドレス学習テーブル１０８及び状態変更指示パケット処理手段１０９を備える。ネットワークインターフェース１０２～１０７には、それぞれを一意に識別するために名前（図ではＡ～Ｆ）が割り当てられている。なお、名前は、一意に識別できれば番号等を用いてもよい。

【００３１】

これらのネットワークインターフェース１０２～１０７は、それぞれ異なるネットワークと接続されており、パケットの送受信を行う。なお、本実施の形態では、ネットワークとしてＩＥＥＥで規定されているＣＳＭＡ／ＣＤ型の８０２．３ネットワークを、ツイストペア線で接続することを想定しているが、本発明は、その他のネットワーク（例えば無線ネットワーク）にも適用可能である。

【００３２】

パケット中継手段１０１は、全てのネットワークインターフェース１０２～１０７と接続されており、ＯＳＩ（Open System Interconnection）モデルのデータリンク層でパケット中継を行う。アドレス学習テーブル１０８には、パケット中継手段１０１がパケットを送信すべきネットワークインターフェースを判断するために必要な情報が格納されている。

【００３３】

図３は、アドレス学習テーブル１０８の構成図（１）である。

アドレス学習テーブル１０８の各エントリは、アドレスフィールド３０１と送信ポートフィールド３０２を含む。アドレスフィールド３０１には、物理アドレス（以下、ＭＡＣアドレスと表記する）が、送信ポートフィールド３０２には、ネットワークインターフェースの名前が、それぞれ格納される。ここで、アドレス学習テーブル１０８の各エントリは、パケットを中継する際、パケットの宛先

アドレスがアドレスフィールド３０１に一致した場合、同じエントリの送信ポートフィールド３０２で示されるネットワークインターフェースから、パケットを送信することを表している。なお、送信ポートフィールド３０２には、複数のネットワークインターフェースを登録することができる。例えば、特殊なケースとして、ＬＡＮスイッチ１００自体のアドレスをアドレスフィールド３０１に登録し、送信ポートフィールド３０２を「X」とした場合、このエントリは、該当するパケットを、ＬＡＮスイッチ１００宛のパケットとして処理することを示している。

【００３４】

状態変更指示パケット処理手段１０９は、ＬＡＮスイッチ１００に接続されたいずれかのネットワークを介して、外部（例えば、後述する認証サーバ４０１）よりＬＡＮスイッチ１００宛に送られた状態変更指示パケットを、パケット中継手段１０１を介して受信すると共に、この状態変更指示パケットの内容を適当なネットワークインターフェース１０２～１０７に通知する。状態変更指示パケットは、特定のネットワークインターフェースの状態を特定の状態に変更する指示を情報として保持している。なお、プロトコルとしては、例えば、ＳＮＭＰ（Simple Network Management Protocol）を使用するが、他にもｔｅｌｎｅｔ（telecommunications network protocol）やＨＴＴＰ（Hyper Text Transfer Protocol）などのプロトコルを利用してもよい。また、本実施の形態では、ネットワーク間接続装置としてＬＡＮスイッチ１００を使用しているが、ルータ等その他のネットワーク間接続装置に対しても、本発明は適用可能である。

【００３５】

図２は、ネットワークインターフェース１０２～１０７の構成図である。

ネットワークインターフェース１０２～１０７は、例えば、ネットワークに接続するための物理インターフェース２０１、ネットワークが使用可能であるかどうかを検出する回線断検出手段２０２及びネットワークインターフェースの状態を管理する状態管理手段２０３を備え、物理インターフェース２０１と状態管理手段２０３は、パケット中継手段１０１にそれぞれ接続されている。

【００３６】

回線断検出手段２０２は、ネットワークの回線（ケーブル）が接続されているかどうか、又は回線を介して接続されている端末が使用可能な状態（電源投入状態）であるかどうかを電気的に検出すると共に、検出された回線断を状態管理手段２０３に通知する。また、本実施の形態では、回線断の検出にあたって、物理インターフェース２０１から通知されるリンクダウン状態が１００ｍｓ以上続いた場合に、回線断と判定している。なお、回線として光ファイバを用いている場合は光信号の有無が、無線ならば電波の有無がそれぞれ同様に回線断の検出に使用できる。

【００３７】

状態管理手段２０３は、ネットワークインターフェースの状態が「接続状態」、「非接続状態」及び「状態なし」のいずれであるかを管理する。ユーザ（スイッチ管理者）は、各ネットワークインターフェース１０２～１０７の状態管理手段２０３に対して、常に「接続状態」または「状態なし」になるように予め設定することができる。各ネットワークインターフェース１０２～１０７の状態は、ユーザによる設定があればそのように、設定がなければ「非接続状態」となる。また、回線断検出手段２０２により回線断が状態管理手段２０３に通知されると、ユーザによる事前の設定がない場合、該当するネットワークインターフェースの状態は「非接続状態」になる。さらに、状態変更指示パケット処理手段１０９による指示があった場合、その指示に基づいて上述の三つの状態のいずれかに変更される。

【００３８】

つぎに、図４のネットワークを例に、本発明に関するネットワーク間接続装置を用いたネットワークの動作を説明する。

図４は、本発明に関するＬＡＮ１００を用いたネットワークの構成図である。

このネットワークは、例えば、ＬＡＮスイッチ１００（アドレス２２：２２：００：ＦＦ：ＦＦ：ＦＦ）と、ＬＡＮスイッチ１００のネットワークインターフェースＡ１０２に接続された認証サーバ４０１（アドレス２２：２２：００：１１：１１：１１）と、ネットワークインターフェースＢ１０３に接続されたファイルサーバ４０２（アドレス２２：２２：００：２２：２２：２２）と、ネット

ワークインターフェースＣ１０４～Ｆ１０７にそれぞれ接続され、ユーザが端末を自由に接続してネットワークを利用できる、いわゆる情報コンセント４０９と、情報コンセント４０９を介してネットワークインターフェースＣ１０４に接続されたユーザ端末４０３（アドレス２２：２２：ＦＦ：００：００：０１）とを備える。

【００３９】

認証サーバ４０１は、ユーザがネットワークの使用を許可されているかどうかを判断し、その結果をＬＡＮスイッチ１００に通知する。本実施の形態では、ユーザの認証を、ユーザＩＤとパスワードを用いて行う。また、ＬＡＮスイッチ１００の各ネットワークインターフェースＣ１０２～Ｆ１０７の設定は、ネットワークインターフェースＢ１０３は常に「接続状態」、ネットワークインターフェースＡ１０２は「状態なし」にそれぞれ設定し、ネットワークインターフェースＣ１０４～Ｆ１０７は特に設定をしない。したがって、ネットワークインターフェースＣ１０４～Ｆ１０７は、初期化時に「非接続状態」となる（なお、この際、ＬＡＮスイッチ１００の学習テーブル１０８は、図３に示すようになっている。）。

【００４０】

つぎに、このネットワークで、ユーザ端末４０３（アドレス２２：２２：ＦＦ：００：００：０１）がネットワークインターフェースＣ１０４につながる情報コンセント４０９に接続された場合について説明する。

図５は、ユーザ端末４０３を情報コンセント４０９に接続した際の通信シーケンス図である。

まず、認証を受けていないユーザ端末４０３が、ファイルサーバ４０２にアクセスする場合、ユーザ端末４０３から、宛先アドレスがファイルサーバ４０２のアドレス（２２：２２：００：２２：２２：２２）、かつ、送信元アドレスがユーザ端末４０３のアドレス（２２：２２：ＦＦ：００：００：０１）であるファイルサーバ宛パケット５０１が送信される。ここで、パケット５０１を受信したＬＡＮスイッチ１００の中継処理を説明する。

【００４１】

図６は、パケット受信に対するＬＡＮスイッチ１００の中継処理を示すフローチャートである。

まず、パケット５０１の送信元アドレス（ユーザ端末４０３のアドレス２２：２２：ＦＦ：００：００：０１）を学習テーブル１０８に登録する。また、送信ポートフィールド３０２として登録されるネットワークインターフェースはＣとなる。

【００４２】

図７は、アドレス学習テーブル１０８の構成図（２）である。

学習テーブル１０８のエントリ＃４には、上述のように送信元アドレスとして、ユーザ端末４０３のアドレスが登録され、送信ポートとして、ネットワークインターフェースＣがそれぞれ登録される。

【００４３】

つぎに、ファイルサーバ４０２の宛先アドレス（２２：２２：００：２２：２２：２２）が学習テーブル１０８に登録済みであるので（処理６０２）、学習テーブル１０８の送信ポートフィールド３０２の内容に基づいて、を送信ポートＢを取得すると共に（処理６０３）、中継処理を行う（処理６０４）。

【００４４】

ここで、処理６０４について説明する。

図８は、処理６０４のフローチャートである。

まず、送信ポート（この場合ネットワークインターフェースＢ１０３）と受信ポート（この場合ネットワークインターフェースＣ１０４）とが同一かどうかを判定する（処理８０１）。ここでは、送信ポートと受信ポートは異なるポートであるので、後述する中継テーブル９０１に基づいて、パケット中継を行う（処理８０２）。

【００４５】

図９は、中継テーブル９０１の構成図である。

中継テーブル９０１は、受信ポートの状態と送信ポートの状態に基づいて、パケットの中継／廃棄を判定するためのテーブルである。ここでは、ユーザ端末４０３から送信されたパケット５０１を受信するＬＡＮスイッチ１００の受信ポー

ト（ネットワークインターフェースＣ１０４）は「非接続状態」であり、送信ポート（ネットワークインターフェースＢ１０３）は「接続状態」であるので、中継テーブル９０１により「廃棄」の結果が得られる。このため、パケット５０１は廃棄される。これにより、認証を受けていないユーザ端末４０３からのファイルサーバ４０２へのアクセスは回避されたことになる。

【００４６】

さらに、続いて、ユーザ端末４０３が、認証サーバ４０１に認証サーバ宛パケット５０２を送信する場合について説明する。ユーザ端末４０３が、宛先アドレスが認証サーバ４０１のアドレス（２２：２２：００：１１：１１：１１）であり、かつ、送信元アドレスがユーザ端末４０３のアドレス（２２：２２：ＦＦ：００：００：０１）であるパケット５０２を送信する。このパケット５０２を受信したＬＡＮスイッチ１００は、上述した図６に従い中継処理を行う。

【００４７】

まず、学習テーブル１０８には、先のパケット５０１受信時、アドレス（２２：２２：ＦＦ：００：００：０１）が既に登録されているので、処理６０１を通過する。つぎに、宛先アドレス（２２：２２：００：１１：１１：１１）が学習テーブル１０８に登録済みであるので（処理６０２）、送信ポートフィールド３０２の内容に基づいて、送信ポート（Ａ）から中継処理を行う（処理６０４）。

【００４８】

ここで、再び、図８及び９を用いて処理６０４について説明する。

まず、送信ポート（Ａ）が受信ポート（Ｃ）とは異なるので（処理８０１）、処理８０２に進む。受信ポートの状態は「非接続状態」、送信ポートの状態は「状態なし」であるので、中継テーブル９０１より「中継」の結果が得られる。このため、パケット５０２はネットワークインターフェースＡ１０２から認証サーバ４０１に中継される。

【００４９】

さらに、認証サーバ４０１からユーザ端末４０３への応答のパケット５０３は、同様の中継処理により、受信ポートが「状態なし」、送信ポートが「非接続状態」であるので、「中継」となる。つまり、認証サーバ４０１とユーザ端末４０

３との間で双方向の通信が成立することになり、ユーザの認証が行える。

【００５０】

認証サーバ４０１では、例えば、ユーザ端末４０３から送られてきたユーザＩＤ及びパスワード５０４がネットワークの使用許可を与えられたユーザのものと一致した場合、ＬＡＮスイッチ１００に対して接続許可を通知する。この接続許可の通知には、宛先アドレスがＬＡＮスイッチ１００のアドレス（２２：２２：００：ＦＦ：ＦＦ：ＦＦ）である状態変更指示パケット５０５を送信する。パケット５０５には、「接続状態への状態変更」とユーザ端末４０３のアドレス（２２：２２：ＦＦ：００：００：０１）が情報として含まれている。

【００５１】

状態変更指示パケット５０５を受信したＬＡＮスイッチ１００は、学習テーブル１０８により、宛先アドレスに対応する送信ポートフィールド３０２が「Ｘ」であるので（処理６０２）、パケット５０５は、状態変更指示パケット処理手段１０９に送られる（処理６０５）。状態変更指示パケット処理手段１０９は、パケット５０５に含まれる情報からユーザ端末４０３のアドレス（２２：２２：ＦＦ：００：００：０１）を取得すると共に、このアドレスを学習テーブル１０８のアドレスフィールド３０１から検索する。この検索で得られたエントリの送信ポートフィールド３０２に示されたネットワークインターフェース（この場合はＣ）に対して、状態を「接続状態」に変更するように指示する。

【００５２】

ネットワークインターフェースＣ１０４の状態が「接続状態」に変更されることで、ユーザ端末４０３からファイルサーバ宛パケット５０６を送信する場合、受信ポートが「接続状態」であり、かつ、送信ポートが「接続状態」であるため、中継テーブル９０１により「中継」となる。これにより、ユーザ端末４０３からファイルサーバ４０２へのアクセスが可能となる。

【００５３】

次に、ユーザ端末４０３が情報コンセント４０９から離脱した場合のＬＡＮスイッチ１００の動作を説明する。

ユーザ端末４０３が情報コンセント４０９からケーブル（ツイストペア線）を

抜いて接続を解除すると、ネットワークインターフェースＣ１０４の物理インターフェース２０１が回線断の状態になる。その状態で１００ｍｓが経過すると、回線断検出手段２０２は、状態管理手段２０３に回線断を通知する。回線断を通知された状態管理手段２０３は、ネットワークインターフェースＣ１０４の状態を「非接続状態」に変更する。これにより、新たなユーザ端末が同じ情報コンセント４０９に接続された場合でも、あらためて認証を受けるまではファイルサーバ４０２にアクセスできなくなる。

【００５４】

以上のように、本実施の形態のＬＡＮスイッチ１００を用いることで、認証前のユーザ端末４０３からは、ファイルサーバ４０２へのアクセスが阻止され、認証後はアクセスが可能になり、さらに、ユーザ端末４０３の離脱後は、再び認証を行うまではファイルサーバ４０２へのアクセスが阻止されるネットワークシステムを構築することができる。また、本実施の形態では、ユーザ端末４０３がネットワークインターフェースＣ１０４につながる情報コンセント４０９に接続された場合について説明したが、ネットワークインターフェースＣ１０４～Ｆ１０７の動作は同様であり、ユーザ端末４０３が任意の情報コンセント４０９に接続されても同様の効果が得られる。

【００５５】

また、本実施の形態では、ネットワークインターフェースの状態を、回線断により「非接続状態」に再初期化したが、ユーザが離脱前に認証サーバ４０１と通信して離脱を通知し、その通知を受けた認証サーバ４０１は、「非接続状態に状態変更」とユーザ端末４０３のアドレスとを情報として持つパケットを、ＬＡＮスイッチ１００のアドレス（２２：２２：００：ＦＦ：ＦＦ：ＦＦ）宛に送り、状態変更指示パケット処理手段１０９により、ネットワークインターフェースの状態を「非接続状態」に変更することも可能である。これにより、ユーザは、ユーザ端末４０３と情報コンセント４０９の接続を切らずに、ネットワークの使用可否を制御できる。

【００５６】

（第２の実施の形態）

図１０は、本発明に関するネットワーク間接続装置の第２の実施の形態の構成図である。

ルータ１０００は、例えば、複数の物理インターフェース１００２～１００７、パケット中継手段１００１、複数のフィルタリング処理部１０１２～１０１７及びフィルタリング変更指示処理手段１００９を備える。物理インターフェース１００２～１００７は、それぞれ異なるネットワークと接続されており、パケットの送受信を行う。パケット中継手段１００１は、ＩＰ(Internet Protocol)プロトコルに基づいたパケット中継を行う。なお、本実施の形態では、パケット中継のプロトコルとしてＩＰプロトコルを用いたが、本発明は、例えば、ＩＰｖ６(ＩＰ version 6)など、その他のネットワーク層プロトコル、にも適用可能である。また、本実施の形態では、ネットワーク間接続装置としてルータ１０００を使用しているが、ＬＡＮスイッチ等その他のネットワーク間接続装置に対しても、本発明は適用可能である。

【００５７】

図１１は、フィルタリング処理部１０１２～１０１７の構成図である。

フィルタリング処理部１０１２～１０１７は、フィルタリングテーブル１１０１、パケット処理部１１０２を備える。フィルタリングテーブル１１０１には、パケットの中継または廃棄の判断のための情報が格納されている。パケット処理部１１０２は、フィルタリングテーブル１１０１の情報に基づいて、パケットの廃棄又は、パケット中継手段１００１への送信を行う。パケット中継手段１００１に送られたパケットは、物理インターフェース１００２～１００７に送信される。各フィルタリングテーブル１１０１は、フィルタリング変更指示処理手段１００９と接続されており、フィルタリング変更指示処理手段１００９からの指示に応じてフィルタリングテーブル１１０１の内容を変更することができる。

【００５８】

図１２は、フィルタリングテーブル１１０１の構成図（１）である。

フィルタリングテーブル１１０１は、パケットの中継または廃棄の判断のための情報を格納しており、各エントリは、宛先アドレス条件１２０１、送信元アドレス条件１２０２、中継／廃棄フラグ１２０３を含む。宛先アドレス条件１２０

１及び送信元アドレス条件１２０２には、ＩＰアドレスまたは「任意」が登録されている。中継／廃棄フラグ１２０３には、宛先アドレスと送信元アドレスがそれぞれ宛先アドレス条件１２０１と送信元アドレス条件１２０２に一致した受信パケットを中継すべきか又は廃棄すべきかが登録されている。複数のエントリに一致するパケットの場合は、テーブルの先頭に近いエントリが適用される。また、一致するエントリが一つもないパケットは、パケット中継手段１００１に送られる。

【００５９】

フィルタリング変更指示処理手段１００９は、認証サーバ１３１１とネットワークを介して通信し、認証サーバ１３１１からフィルタリング変更指示を受ける。本実施の形態では、通信プロトコルとしてｔｅｌｎｅｔを想定するが、ＨＴＴＰやＣＯＰＳ（Common Open Policy Service）などのプロトコルを使用してもよい。フィルタリング変更指示は、対象とするエントリの内容と、追加／削除の指示を保持している。フィルタリング変更指示処理手段１００９は、送信元アドレス条件のＩＰアドレスが属するサブネットに接続された物理インターフェース１００２～１００７に対応するフィルタリング処理部１０１２～１０１７のフィルタリングテーブル１１０１にその指示を反映させる。

【００６０】

図１３は、本発明に関するルータ１０００を用いたネットワークの構成図である。

このネットワークは、例えば、ルータ１０００の各物理インターフェース１００２～１００７はそれぞれ接続されているサブネットＡ１３０２～Ｆ１３０７と、サブネットＡ１３０２接続されている認証サーバ１３１１と、サブネットＢ１３０３に接続されているファイルサーバ１３２２と、サブネットＣ１３０４～Ｆ１３０７にそれぞれ接続され、ユーザが自由に端末を接続できる複数の情報コンセント４０９と、情報コンセント４０１を介してサブネットＣ１３０４に接続されているユーザ端末１３３３とを備えている。

【００６１】

各フィルタリングテーブル１１０１の初期状態での内容は、フィルタリング処

理部Ａ１０１２、Ｂ１０１３では何も登録されておらず、フィルタリング処理部Ｃ１０１４～Ｆ１０１７では、上述の図１２の内容が設定されているものとする。

【００６２】

つぎに、このネットワークで、ユーザ端末１３３３をサブネットＣ１３０４の情報コンセント４０９に接続した場合について説明する。

図１４は、ユーザ端末１３３３を情報コンセント４０９に接続した際の通信シーケンス図である。

認証を受けていないユーザ端末１３３３が、ファイルサーバ１３２２にアクセスするためにファイルサーバ１３２２のＩＰアドレス（１９２．１６８．２．２）宛のファイルサーバ宛パケット１４０１を送信した場合、パケット１４０１は、ルータ１０００の物理インターフェースＣ１００４を介して、フィルタリング処理部Ｃ１０１４に送られる。フィルタリング処理部Ｃ１０１４のフィルタリングテーブル１１０１のうちパケット１４０１に該当するエントリは、＃２のエントリであるので、パケット１４０１を廃棄する。したがって、ユーザ端末１３３３の送信するパケット１４０１は、ファイルサーバ１３２２に到達することはない。

【００６３】

つぎに、ユーザ端末１３３３が認証を受けてファイルサーバ１３２２にアクセスする場合の動作を説明する。

ユーザ端末１３３３は、認証を受けるために認証サーバ１３１１のＩＰアドレス（１９２．１６８．１．１）宛のパケット１４０２を送信する。ルータ１０００の物理インターフェースＣ１００４からフィルタリング処理部Ｃ１０１４に送られたパケット１４０２に対して、フィルタリングテーブル１１０１の検索が行われる。この場合、フィルタリングテーブル１１０１のエントリ＃１、＃２の両方が該当するので、テーブル内で先に登録されている＃１が適用される。このため、パケット１４０２は、パケット中継手段１００１に送られる。

【００６４】

したがって、ユーザ端末１３３３から認証サーバ１３１１への通信が成立する

。認証サーバ１３１１からユーザ端末１３３３への応答パケット１４０３は、物理インターフェースＡ１００２からフィルタリング手段Ａ１０１２に送られる。フィルタリング手段Ａ１０１２のフィルタリングテーブル１１０１には何も登録されていないため、パケット１４０３は中継される。このため、ユーザ端末１３３３と認証サーバ１３１１との双方向の通信が成立することになり、ユーザ端末１３３３は、認証を受けることができる。

【００６５】

認証サーバ１３１１は、ユーザ端末１３３３から送られてきたユーザＩＤとパスワード１４０４がネットワーク接続を許可されたユーザのものと一致した場合、ルータ１０００のフィルタリング変更指示処理手段１００９と通信すると共に、フィルタリングテーブル１１０１に、宛先アドレス条件が「任意」、送信元アドレス条件がユーザ端末１３３３のアドレスである「１９２．１６８．３．３」、中継／廃棄フラグが「中継」であるエントリを追加することを、ルータ１０００に対して指示１４０５する。

【００６６】

図１５は、フィルタリングテーブル１１０１の構成図（２）である。

変更指示処理手段１００９は、送信元アドレス条件「１９２．１６８．３．３」が属するサブネット（サブネットＣ１３０４）が物理インターフェースＣ１００４に接続されているので、フィルタリング手段１３１４のフィルタリングテーブル１１０１に対して、エントリを追加する。その結果、フィルタリング手段Ｃ１０１４のフィルタリングテーブル１１０１には、エントリ＃１～＃３までが登録されていることになる。

【００６７】

この状態で、ユーザ端末１３３３がファイルサーバ宛パケット１４０６を送信すると、フィルタリング手段Ｃ１０１４のフィルタリングテーブル１１０１のエントリ＃１が該当するため、パケット１４０６は中継されることになり、ファイルサーバ１３２２へのアクセスが可能となる。

【００６８】

以上のように、本実施の形態のルータ１０００を用いることで、認証前のユー

ザ端末１３３３からファイルサーバ１３２２へのアクセスが阻止され、認証後はアクセスが可能になるネットワークを構築することができる。また、本実施の形態では、ルータ１０００のネットワークインターフェースで複数の情報コンセント４０９を扱うことができ、さらに、ネットワークインターフェースごとに個別のフィルタリング手段を設けることにより、フィルタリング処理の負荷を分散することができる。

【００６９】

（第３の実施の形態）

図１６は、本発明に関するネットワーク間接続装置の第３の実施の形態の構成図である。

ＬＡＮスイッチ１６００は、例えば、パケット中継手段１６０１、複数のネットワークインターフェース１６０２～１６０５、アドレス学習テーブル１６０６、フィルタリングテーブル１６０７及び状態変更指示パケット処理手段１６０８を備える。ネットワークインターフェース１６０２～１６０５には、各々を一意に識別するために名前（図ではＡ～Ｄ）が割り当てられている。なお、名前は、一意に識別できれば番号等を用いてもよい。

【００７０】

これらのネットワークインターフェース１６０２～１６０５は、それぞれ異なるネットワークに接続されており、パケットの送受信を行う。なお、本実施の形態でのネットワークは、ＩＥＥＥの８０２．３ネットワークを用いるようにした。また、以下の本実施の形態を説明では、ネットワークインターフェースＡ１６０２を「アップリンク」、ネットワークインターフェースＢ１６０３～Ｄ１６０５を「ダウンリンク」と称する。

【００７１】

パケット中継手段１６０１は、アドレス学習テーブル１６０６とフィルタリングテーブル１６０７の情報に基づいて、ネットワーク間でのパケット中継を行う。状態変更指示パケット処理手段１６０８は、後述する認証サーバ１９０１からの状態変更指示パケットを受信すると共に、フィルタリングテーブル１６０７と学習テーブル１６０６の内容を変更する。状態変更指示パケットには、ＩＰアド

レスと「許可／禁止」が情報として保持されている。

【００７２】

図１７は、フィルタリングテーブル１６０７の構成図である。

フィルタリングテーブル１６０７には、中継を許可していないパケットを識別するための情報が登録されている。フィルタリングテーブル１６０７の各エントリは、ＭＡＣアドレスフィールド１７０１、ＩＰアドレスフィールド１７０２、接続ポートフィールド１７０３を含む。ＭＡＣアドレスフィールド１７０１には、フィルタリング対象となるＭＡＣアドレスが、ＩＰアドレスフィールド１７０２には、そのＭＡＣアドレスに対応するＩＰアドレスが、接続ポートフィールド１７０３には、そのＭＡＣアドレスを持つ端末が属するネットワークが接続されているネットワークインターフェース１６０２～１６０５の名前が、それぞれ登録されている。

【００７３】

図１８は、学習テーブル１６０６の構成図（１）である。

学習テーブル１６０６には、パケットの中継先ネットワークインターフェースに関する情報が登録されている。学習テーブル１６０６の各エントリは、ＭＡＣアドレスフィールド１８０１及び接続ポートフィールド１８０２を含む。ＭＡＣアドレスフィールド１８０１には、中継対象のＭＡＣアドレスが、接続ポートフィールド１８０２には、宛先ＭＡＣアドレスがＭＡＣアドレスフィールドに一致したパケットを中継すべきネットワークインターフェース１６０２～１６０５の名前が、それぞれ登録されている。また、一定時間利用されなかったエントリは、自動的に学習テーブル１６０６から削除されるように設定されている。なお、本実施の形態では、ネットワーク間接続装置としてＬＡＮスイッチ１６００を使用しているが、ルータ等その他のネットワーク間接続装置に対しても、本発明は適用可能である。

【００７４】

次に、図１９のネットワークを例に、本発明に関するＬＡＮスイッチ１６００を用いたネットワークの動作を説明する。

図１９は、本発明に関するＬＡＮスイッチ１６００を用いたネットワークの構

成図である。

このネットワークは、例えば、ＬＡＮスイッチ１６００と、ＬＡＮスイッチ１６００の各ネットワークインターフェース１６０２～１６０５にそれぞれ接続されたネットワークＡ～Ｄと、ネットワークＢ～Ｄを介して、ダウンリンクの各ネットワークインターフェースＢ１６０３～Ｄ１６０５に接続された、ユーザが自由に端末を接続できる複数の情報コンセント４０９と、情報コンセント４０９を介してネットワークＢに接続されたユーザ端末１９０５と、アップリンクのネットワークＡに接続されたルータ１９０４と、ネットワークを介してルータ１９０４に接続された、ファイルサーバ１９０２、ＤＨＣＰサーバ１９０３、認証サーバ１９０１とを備える。

【００７５】

ルータ１９０４は、ＢＯＯＴＰリレーエージェント機能を備えると共に、ＩＰプロトコルに基づいた中継を行う。ＤＨＣＰサーバ１９０３は、ＤＨＣＰプロトコルに基づきユーザ端末にＩＰアドレスを配布する。認証サーバ１９０１は、ユーザ認証の結果を状態変更指示パケットにしてＬＡＮスイッチ１６００に通知する。

【００７６】

つぎに、初期状態で、ユーザ端末１９０５をネットワークＢの情報コンセント４０９に接続した場合について説明する。

図２０は、ユーザ端末１９０５をネットワークＢの情報コンセント４０９に接続した際の通信シーケンス図である。

初期状態では、ＬＡＮスイッチ１６００のフィルタリングテーブル１６０７には、何も登録されていない。また、学習テーブル１６０６のＭＡＣアドレス１８０１には、ルータ１９０４のＭＡＣアドレス（２２：２２：００：４４：４４：４４）が、同じく接続ポート１８０２には、ネットワークインターフェースＡ１６０２が、それぞれ登録されている。

【００７７】

まず、ユーザ端末１９０５は、情報コンセント４０９に接続されると、ＤＨＣＰプロトコルによりＩＰアドレスを要求するためのアドレス要求パケット２００

１を、ブロードキャストアドレス宛に送信する。ここで、パケット２００１を受信したＬＡＮスイッチ１６００の中継処理を説明する。

【００７８】

図２１は、パケット受信に対するＬＡＮスイッチ１６００の中継処理を示すフローチャートである。

ここでは、パケット２００１の宛先アドレスは、学習テーブル１６０６に登録なしであり（処理２１０１）、かつ、ブロードキャストアドレスである（処理２１０２）。また、受信ポートはネットワークインターフェースＢ１６０３で、アップリンクではない（処理２１０３）。さらに、送信元ＭＡＣアドレスが学習テーブル１６０６にない（処理２１０４）。また、フィルタリングテーブル１６０７に送信元ＭＡＣアドレスがないことから、ユーザ端末１９０５のアドレス（２２：２２：ＦＦ：００：００：０１）をフィルタリングテーブル１６０７に登録する（処理２１０５）。

【００７９】

ここで、フィルタリングテーブル１６０７では、図１７に示すように、ＩＰアドレス１７０２に「未登録」、接続ポート１７０３に「Ｂ」がそれぞれ登録される。これにより、パケット２００１は、アップリンクにのみ中継され、ルータ１９０４に送られる（処理２１０５）。

ここで、再び通信シーケンスの説明をする。パケット２００１は、ＤＨＣＰパケットであるので、ルータ１９０４のＢＯＯＴＰリレーエージェント機能により、ＤＨＣＰサーバ１９０３に中継される。ＤＨＣＰサーバ１９０３からのアドレス配布パケット２００２は、ルータ１９０４のＢＯＯＴＰリレーエージェント機能により、ユーザ端末１９０５のＭＡＣアドレス（２２：２２：ＦＦ：００：００：０１）宛に送られる。

【００８０】

ＬＡＮスイッチ１６００は、パケット２００２を中継処理する。ここで、上述のフローチャートの説明に戻る。パケット２００２は、宛先ＭＡＣアドレスが学習テーブル１６０７になく（処理２１０１）、かつ、宛先がブロードキャストではない（処理２１０２）。また、フィルタリングテーブル１６０７に宛先があり

（処理２１０６）、かつ、受信ポートがネットワークインターフェースＡ１６０２であり、アップリンクである（処理２１０７）。さらに、プロトコルがＩＰであり（処理２１０８）、送信元ＩＰアドレスがリレーエージェント（ルータ１９０４）のＩＰアドレスである（処理２１０９）。

【００８１】

フィルタリングテーブル１６０７のエントリ＃１により、接続ポート１７０３がネットワークインターフェースＢ１６０３であることがわかるので、パケット２００２をネットワークインターフェースＢ１６０３から送信する（処理２１１０）。これにより、ユーザ端末１９０５にアドレス配布パケット２００２が送られることになる。ここで、ユーザ端末１９０５に、ＤＨＣＰサーバ１９０３から配布されたアドレスを「１９２．１６８．５．１」とする。

【００８２】

ここで、ユーザ端末１９０５が認証を受けずにファイルサーバ１９０２にアクセスを試みる場合について説明する。但し、アクセスのためのプロトコルはＩＰを用いる。

まず、ファイルサーバ１９０２（アドレス１９２．１６８．１．２）とユーザ端末１９０５（アドレス１９２．１６８．５．１）ではＩＰサブネットが異なるので、ファイルサーバ１９０２にアクセスするためのパケット２００３は、宛先ＩＰアドレスがファイルサーバ１９０２の（１９２．１６８．１．２）で、宛先ＭＡＣアドレスがルータ１９０４の（２２：２２：００：４４：４４：４４）である。

【００８３】

ここで、ファイルアクセスパケット２００３を受信したＬＡＮスイッチ１６００の処理を説明する。

まず、宛先ＭＡＣアドレスが学習テーブル１６０６に登録されている（処理２１０１）。送信元ＭＡＣアドレスがフィルタリングテーブル１６０７に登録されており、送信元ＩＰアドレスであって、ＤＨＣＰサーバ１９０３からユーザ端末１９０５に配布されたＩＰアドレス（１９２．１６８．５．１）を「未登録」であったＩＰアドレスフィールド１７０２に登録する（処理２１１１）。これによ

り、パケット２００３は、ＩＰの仕様に基づいて中継されることになり、ルータ１９０４を経由して、ファイルサーバ１９０２に送信されると共に、ファイルサーバ１９０２からの応答としてデータパケット２００４が送られる。

【００８４】

ここで、パケット２００４を受信したＬＡＮスイッチ１６００の処理について説明する。

ルータ１９０４を経由してＬＡＮスイッチ１６００に送られたパケット２００４は、宛先ＭＡＣアドレスが学習テーブル１６０６になく（処理２１０１）、かつ、宛先がブロードキャストでもない（処理２１０２）。また、フィルタリングテーブル１６０７に登録があり（処理２１０６）、かつ、受信ポートがネットワークインターフェースＡであり、アップリンクである（処理２１０７）。さらに、プロトコルがＩＰ（処理２１０８）であり、送信元ＩＰアドレスがファイルサーバのアドレスなので廃棄される（処理２１０９）。したがって、パケット２００４は、ユーザ端末１９０５に届かないため、アクセスは成立しない。

【００８５】

つぎに、ユーザ端末１９０５が認証を行う場合について説明する。

まず、ユーザ端末１９０５からユーザＩＤとパスワードパケット２００５が認証サーバ１９０１に送られる。認証サーバ（アドレス１９２．１６８．１．１）とユーザ端末１９０５（アドレス１９２．１６８．５．１）では属するサブネットが異なるので、パケット２００５の宛先ＩＰアドレスは、認証サーバ１９０１のＩＰアドレスであり、宛先ＭＡＣアドレスは、ルータ１９０４のＭＡＣアドレスとなる。

【００８６】

ここで、パケット２００５を受信したＬＡＮスイッチ１６００の処理について説明する。ＬＡＮスイッチ１６００では、宛先ＭＡＣアドレスが学習テーブル１６０６に登録済みであるので（処理２１０１）、パケット２００５を認証サーバ１９０１に中継する。

【００８７】

認証サーバ１９０１では、ユーザ端末１９０５から送られたユーザＩＤとパス

ワードがネットワークの使用を許可されたユーザのものであった場合、状態変更指示通知パケット２００６をＬＡＮスイッチ１６００の状態変更指示通知パケット処理手段１６０９に送信する。このパケット２００６には、ＩＰアドレス（１９２．１６８．５．１）と「許可」が情報として含まれる。この状態変更指示通知パケット２００６を受けた状態変更指示通知パケット処理手段１６０９は、フィルタリングテーブル１６０７からＩＰアドレス（１９２．１６８．５．１）を検索する。

【００８８】

図２２は、学習テーブル１６０６の構成図（２）である。

フィルタリングテーブル１６０７からＩＰアドレス（１９２．１６８．５．１）を検索することで得られたＭＡＣアドレスフィールド１７０１と接続ポートフィールド１７０３とを、新たなエントリとして、学習テーブル１６０６に追加する。

【００８９】

ここで、ユーザ端末１９０５がファイルサーバ１９０２へのアクセスを試みると、上述のように、このファイルアクセスパケット２００７は、ファイルサーバ１９０２に届く。その応答データであるパケット２００８は、ＬＡＮスイッチ１６００で次のように処理される。

【００９０】

パケット２００８の宛先ＭＡＣアドレスは、ユーザ端末１９０５のＭＡＣアドレス（２２；２２：ＦＦ：００：００：０１）であるので、現在の学習テーブル１６０６（図２２）に登録されている（処理２１０１）。したがって、処理２１１１を経て、パケット２００８は中継され、ユーザ端末１９０５に届く。これにより、今回はファイルサーバ１９０２へのアクセスが成立する。

【００９１】

また、ユーザ端末１９０５が一定時間通信をしなかった場合、学習テーブル１６０６のエントリが自動的に削除されるので、再び認証を行うまではファイルサーバ１９０２へのアクセスはできなくなる。また、ＤＨＣＰによるアドレス配布では、通常、配布したアドレスの使用期限を設けている。このため、ＤＨＣＰサ

ーバ１９０３は、アドレス配布２００２を行ってから時間が経過し使用期限が過ぎたら、タイムアウト通知２００９を認証サーバ１９０１に対して行う。タイムアウト通知２００９を受けた認証サーバは、ＩＰアドレスとしてタイムアウトしたアドレス（この場合１９２．１６８．５．１）、および「禁止」という情報を含む状態変更指示通知パケット２０１０をＬＡＮスイッチ１６００の状態変更指示通知パケット処理手段１６０９に送信する。

【００９２】

状態変更指示通知パケット処理手段１６０９は、ＩＰアドレス（１９２．１６８．５．１）をフィルタリングテーブル１６０７から検索し、対応するＭＡＣアドレスフィールド１７０１に登録されたＭＡＣアドレス（この場合２２：２２：ＦＦ：００：００：０１）を、学習テーブル１６０６から検索する。そして、フィルタリングテーブル１６０７と学習テーブル１６０６の双方から該当するエントリを削除する。その結果、ユーザ端末１９０５は、再び認証を受けなければファイルサーバ１９０２にアクセスできなくなる。

【００９３】

以上のように、本実施の形態のＬＡＮスイッチ１６００を用いることで、認証を受けていないユーザ端末１９０５からのファイルサーバ１９０２へのアクセスを防止すると共に、認証を受けたユーザ端末１９０５からのファイルサーバ１９０２へのアクセスを許可するネットワークを構築できる。また、本実施の形態では、一定時間無通信である場合や、アドレスの有効期限が切れた場合に、ＬＡＮスイッチのテーブルを自動的に変更し、再び認証を受けるまではファイルサーバ１９０２へのアクセスを防止することもできる。

【００９４】

（第４の実施の形態）

図２３は、本発明に関するルータ２３００を用いたネットワークの構成図である。

ルータ２３００は、本発明に関するネットワーク間接続装置の第４の実施の形態であり、例えば、複数のネットワークインターフェース２３０２～２３０５、パケット中継手段２３０１、ＩＰアドレス登録表２３０６を備える。

【００９５】

パケット中継手段２３０１は、ＩＰプロトコルに基づいてパケット中継を行い、ＩＰアドレス登録表２３０６に登録されていないアドレスからのパケットに対して、カプセル化処理を行う。ネットワークインターフェースＡ２３０２～Ｄ２３０５は、それぞれ異なるネットワークに接続され、パケットの送受信を行う。ＩＰアドレス登録表２３０６には、認証を受けたユーザ端末のＩＰアドレスが登録される。

【００９６】

また、このネットワークは、例えば、ルータ２３００と、ルータ２３００のネットワークインターフェースＡ２３０２に、ネットワークＡを介して接続された認証サーバ２３１０及びファイルサーバ２３１１と、ネットワークインターフェースＢ２３０３～Ｄ２３０５に、ネットワークＢ～Ｄを介して接続され、ユーザが端末を自由に接続できる複数の情報コンセント４０９と、情報コンセント４０９を介してネットワークＢ２３０３に接続されたユーザ端末２３１２とを備える。認証サーバ２３１０は、ユーザ認証を行うと共に、その結果をルータ２３００に通知し、後述するカプセル化したパケットの送受信を行う。

【００９７】

つぎに、初期状態で、ユーザ端末２３１２をネットワークＢ２３１３に接続した場合について説明する。ここで、図２７は、初期状態でのＩＰアドレス登録表２３０６の構成図である。

図２４は、ユーザ端末２３１２をネットワークＢ２３１３に接続した際の通信シーケンス図である。

まず、ユーザ端末２３１２が認証を受けずにファイルアクセスを試みた場合について説明する。

ルータ２３００は、ユーザ端末２３１２からのファイルアクセスパケット２４００を受信すると共に、このパケット２４００に対して中継処理を行う。

【００９８】

図２５は、パケット受信に対するルータ２３００の中継処理を示すフローチャートである。

パケット２４００の宛先アドレスは、ファイルサーバ２３１１のアドレスであり、ルータのカプセル化アドレスではない（処理2.501）。また、送信元アドレスは、ＩＰアドレス登録表２３０６に登録されていないので（処理２５０２）、パケット２４００は、カプセル化される（処理２５０３）。

【００９９】

ここで、「カプセル化」とは、ＩＰヘッダを含むパケット２４００全体をデータとみなし、このデータに対して、宛先アドレスを認証サーバ２３１０のカプセル化アドレス（１９２．１６８．１００．１００）、送信元アドレスをルータ２３００のカプセル化アドレス（１９２．１６８．１００．１０１）とするＩＰヘッダを付加することで、新たなパケット（カプセル化したパケット）を作成することである。このため、カプセル化したパケットは、元々の宛先アドレス（例えば、ファイルサーバ２３１１のアドレス）に係わらず、認証サーバ２３１０に送信されることになる（処理２５０４）。

【０１００】

ここで、カプセル化されたパケットを受信した認証サーバ２３１０の処理について説明する。

図２６は、パケット受信に対する認証サーバ２３１０の処理を示すフローチャートである。

カプセル化されたパケットの宛先アドレスは、認証サーバのカプセル化アドレスであり（処理２６０１）、かつ、送信元アドレスは、ルータのカプセル化アドレスである（処理２６０２）。したがって、パケット２４００のカプセル化を解除し、元々のパケット２４００を復元する（処理２６０３）。元々のパケット２４００の宛先アドレスは、ファイルサーバ２３１１のアドレスであって、認証サーバ２３１０のアドレスではないので（処理２６０４）、パケットは廃棄される。したがって、認証前のユーザ端末２３１２は、ファイルサーバ２３１１へアクセスすることはできない。

【０１０１】

つぎに、ユーザ端末２３１２が認証を受けるためユーザＩＤとパスワードを含むパケット２４０１を認証サーバ２３１０のアドレス宛に送った場合について、

図２４及び２５を用いて説明する。

パケット２４００を受信したルータ２３００では、パケット２４０１の宛先アドレスがルータのカプセル化アドレスではなく（処理２５０１）、かつ、送信元アドレスがＩＰアドレス登録表２３０６に登録されていない（処理２５０２）。このため、パケット２４０１は、カプセル化されると共に（処理２５０３）、認証サーバ２３１０に送信される（処理２５０４）。

【０１０２】

また、認証サーバ２３１０では、宛先アドレスが認証サーバのカプセル化アドレスであり（処理２６０１）、送信元アドレスがルータ２３００のカプセル化アドレスである（処理２６０２）。このため、パケット２４０１のカプセル化を解除する（処理２６０３）。ここで、元々のパケット２４０１の宛先アドレスは、認証サーバ２３１０のアドレスであるので（処理２６０４）、認証を行う（処理２６０５）。さらに、送られてきたパケット２４０１に含まれるユーザＩＤとパスワードがネットワークの使用許可を与えられたユーザのものと一致したら、認証成功を通知するパケット２４０２をカプセル化して送信する（処理２６０６）。この認証サーバ２３１０でのカプセル化は、宛先アドレスをルータ２３００のカプセル化アドレス（１９２．１６８．１００．１０１）とし、送信元アドレスを認証サーバ２３１０のカプセル化アドレス（１９２．１６８．１００．１００）とする。

【０１０３】

さらに、ルータ２３００では、カプセル化された認証成功の通知パケット２４０２を受信し、宛先アドレスがルータのカプセル化アドレスであり（処理２５０１）、かつ、送信元アドレスは認証サーバのカプセル化アドレスである（処理２５０５）。このため、パケット２４０２のカプセル化を解除すると共に（処理２５０６）、復元したパケット２４０２を中継する（処理２５０７）。

【０１０４】

また、認証サーバ２３１０では、ユーザ端末２３１２の認証が成功すると、ルータ２３００に対して、ＩＰアドレス（１９２．１６８．３．３）の登録を指示するＩＰアドレス登録パケット２４０３を送信する。その結果、ＩＰアドレス登

録表２３０６にＩＰアドレス（１９２．１６８．３．３）が登録される。

【０１０５】

つぎに、ユーザ端末２３１２がファイルサーバ２３１１にアクセスするためのファイルアクセスパケット２４０４を送信する場合について説明する。パケット２４０４の宛先アドレスがルータのカプセル化アドレスではなく（処理２５０１）、送信元アドレスであるユーザ端末２３１２のＩＰアドレス（１９２．１６８．３．３）がＩＰアドレス登録表２３０６に登録されている（処理２５０２）。このため、パケット２４０４は、ファイルサーバ２３１１に中継される（処理２５０８）。

【０１０６】

同様に、ファイルサーバ２３１１からの応答データであるパケット２４０５は、ファイルサーバ２３１１のアドレス（１９２．１６８．１０．２）がＩＰアドレス登録表２３０６に登録されているので、ユーザ端末２３１２に中継される。したがって、認証を受けた後は、ユーザ端末２３１２からファイルサーバ２３１１へのアクセスが可能となる。

【０１０７】

さらに、認証サーバ２３１０は、ユーザ認証が成功した後、定期的にユーザ端末２３１２に対してＩＣＭＰ（Internet Control Message Protocol）のＩＣＭＰエコーリクエスト２４０６を送信し、ユーザ端末２３１２から応答データであるＩＣＭＰエコーリプライ２４０７が返ってくることを確認する。

【０１０８】

ＩＣＭＰエコーリクエスト２４０６を送信してから一定時間以内にユーザ端末２３１２からの応答がない場合、認証サーバ２３１０は、ユーザ端末２３１２のＩＰアドレス（１９２．１６８．３．３）をＩＰアドレス登録表から削除する指示をルータ２３００に送信する。その結果、ユーザ端末２３１２のアドレスは、ＩＰアドレス登録表２３０６から削除され、再び認証を受けるまでは、ユーザ端末２３１２からファイルサーバ２３１１へのアクセスはできなくなる。

【０１０９】

以上のように、本実施の形態のルータ２３００を用いることで、認証を受けて

いないユーザ端末２３１２からファイルサーバ２３１１へのアクセスを防止すると共に、認証を受けたユーザ端末２３１２からのファイルサーバ２３１１へのアクセスを許可するネットワークシステムを構築することができる。また、本実施の形態では、定期的にユーザ端末２３１１からの応答を確認することにより、ユーザ端末２３１１がネットワークから離脱したり、使用を中止した場合、ファイルサーバ２３１１へのアクセス許可を自動的に取り消すことができる。

【０１１０】

【発明の効果】

本発明によると、以上説明した通り、ユーザが任意の時刻及び場所に端末を接続しても、認証を受けたユーザにのみネットワーク上の資源へのアクセスを許可すると共に、認証を受けていない不正なユーザからのネットワーク上の資源へのアクセスを禁止することができる。

【図面の簡単な説明】

【図１】

本発明に関するネットワーク間接続装置の第１の実施の形態の構成図。

【図２】

ネットワークインターフェース１０２～１０７の構成図。

【図３】

アドレス学習テーブル１０８の構成図（１）。

【図４】

本発明に関するＬＡＮ１００を用いたネットワークの構成図。

【図５】

ユーザ端末４０３を情報コンセント４０９に接続した際の通信シーケンス図。

【図６】

パケット受信に対するＬＡＮスイッチ１００の中継処理を示すフローチャート。

【図７】

アドレス学習テーブル１０８の構成図（２）。

【図８】

処理６０４のフローチャート。

【図９】

中継テーブル９０１の構成図。

【図１０】

本発明に関するネットワーク間接続装置の第２の実施の形態の構成図。

【図１１】

フィルタリング処理部１０１２～１０１７の構成図。

【図１２】

フィルタリングテーブル１１０１の構成図（１）。

【図１３】

本発明に関するルータ１０００を用いたネットワークの構成図。

【図１４】

ユーザ端末１３３３を情報コンセント４０９に接続した際の通信シーケンス図。

【図１５】

フィルタリングテーブル１１０１の構成図（２）。

【図１６】

本発明に関するネットワーク間接続装置の第３の実施の形態の構成図。

【図１７】

フィルタリングテーブル１６０７の構成図。

【図１８】

学習テーブル１６０６の構成図（１）。

【図１９】

本発明に関するＬＡＮスイッチ１６００を用いたネットワークの構成図。

【図２０】

ユーザ端末１９０５をネットワークＢの情報コンセント４０９に接続した際の通信シーケンス図。

【図２１】

パケット受信に対するＬＡＮスイッチ１６００の中継処理を示すフローチャー

ト。

【図２２】

学習テーブル１６０６の構成図（２）。

【図２３】

本発明に関するルータ２３００を用いたネットワークの構成図。

【図２４】

ユーザ端末２３１２をネットワークＢ２３１３に接続した際の通信シーケンス図。

【図２５】

パケット受信に対するルータ２３００の中継処理を示すフローチャート。

【図２６】

パケット受信に対する認証サーバ２３１０の処理を示すフローチャート。

【図２７】

初期状態でのＩＰアドレス登録表２３０６の構成図。

【符号の説明】

１００　ＬＡＮスイッチ

１０９　状態変更指示パケット処理手段

２０３　状態管理手段

４０１　認証サーバ

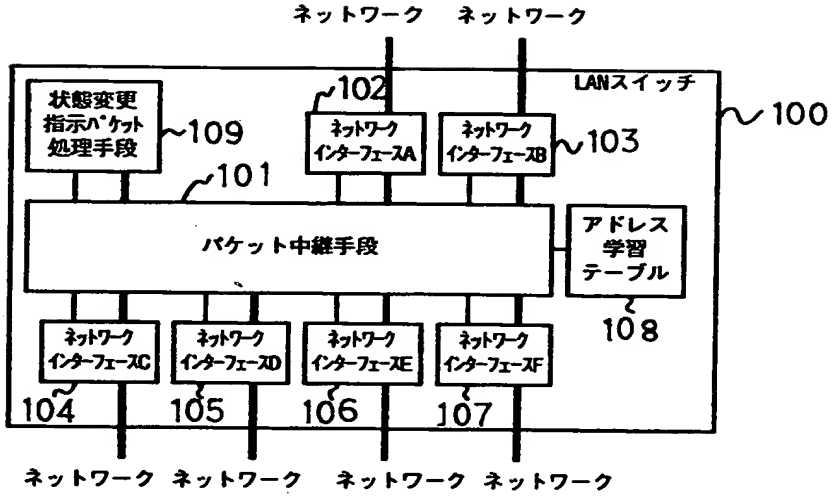
４０２　ファイルサーバ

４０３　ユーザ端末

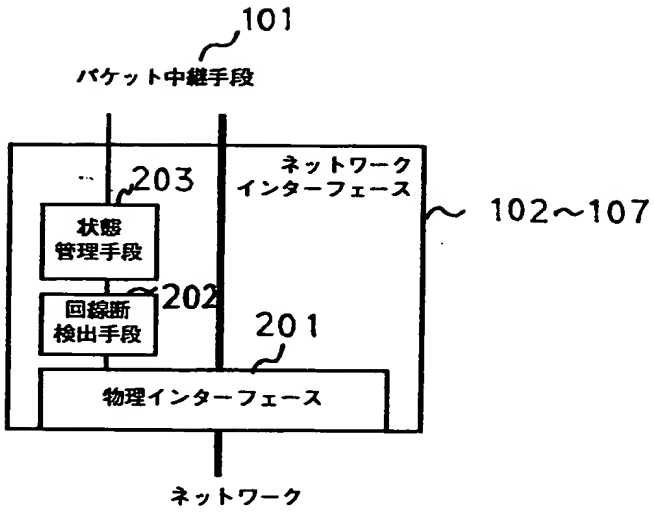
４０９　情報コンセント

【書類名】図面

【図１】


ネットワーク
ネットワーク
LANスイッチ
100
状態変更
指示パケット
処理手段
109
102
ネットワーク
インターフェースA
ネットワーク
インターフェースB
103
101
パケット中継手段
アドレス
学習
テーブル
108
ネットワーク
インターフェースC
ネットワーク
インターフェースD
ネットワーク
インターフェースE
ネットワーク
インターフェースF
104
105
106
107
ネットワーク
ネットワーク
ネットワーク
ネットワーク

【図２】



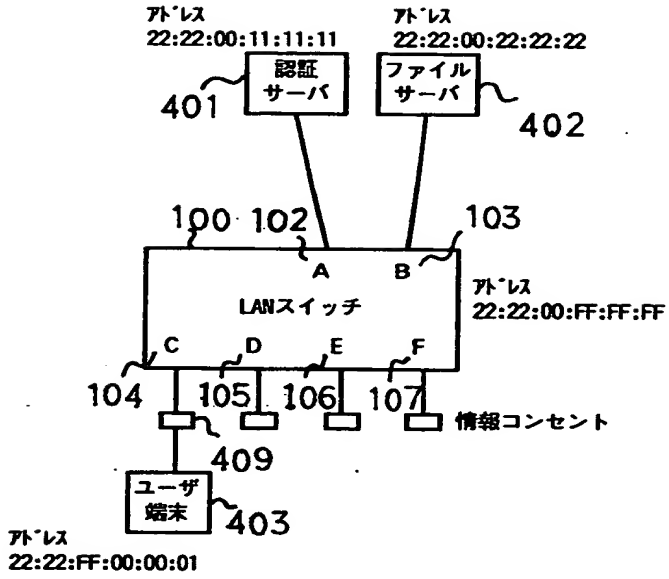
出証特２００１－３０３２４２８

【図３】

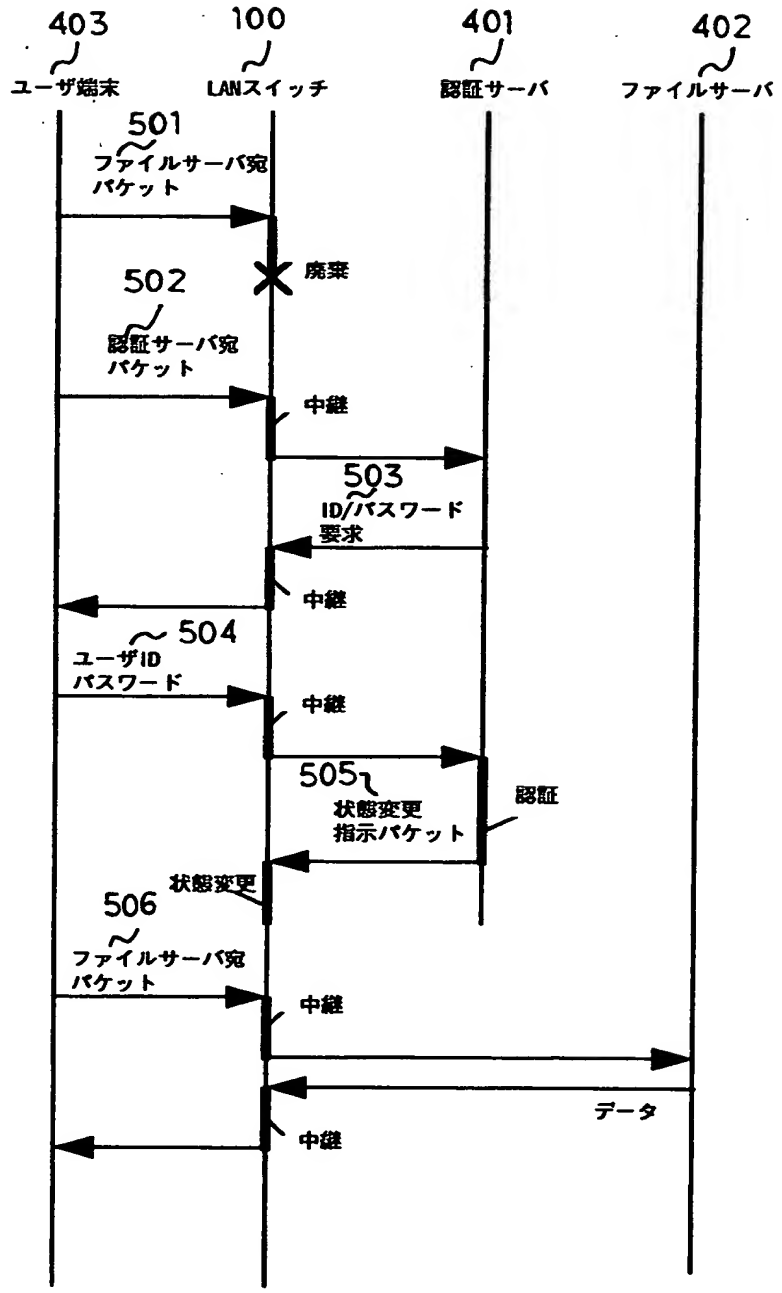
108

#	301 アドレス	302 送信ポート
1	22:22:00:11:11:11	A
2	22:22:00:22:22:22	B
3	22:22:00:FF:FF:FF	X

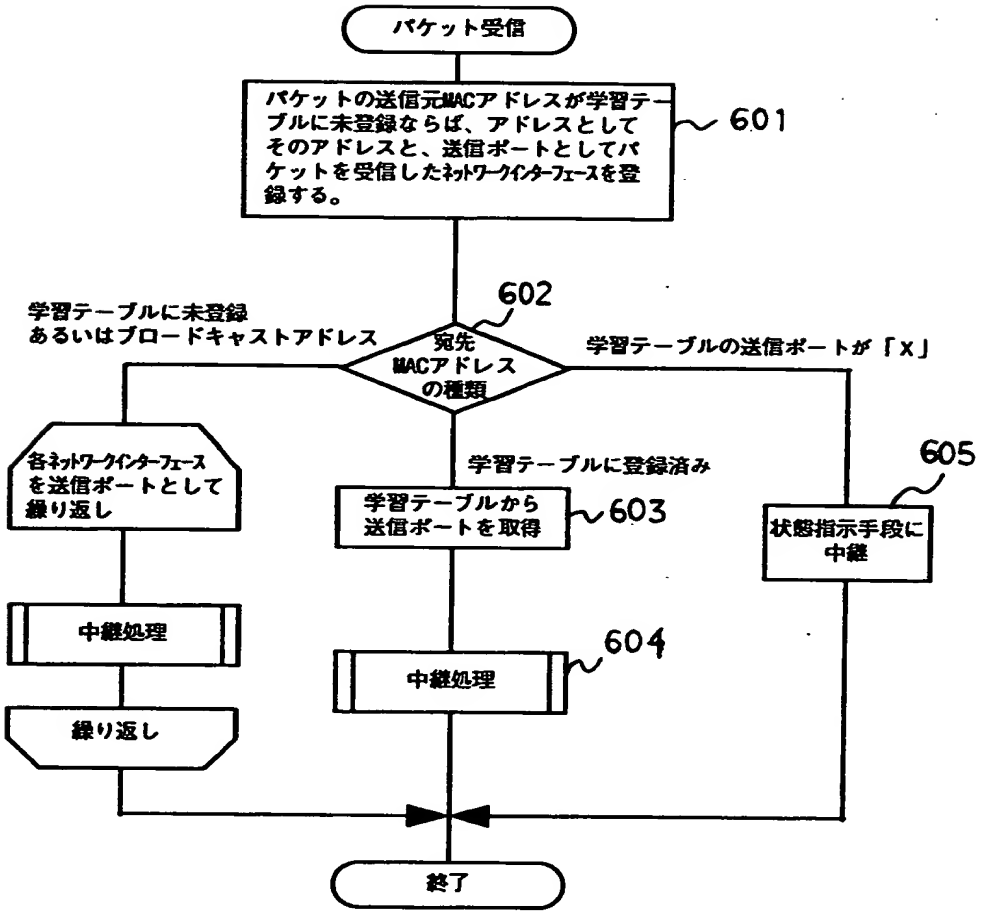
【図４】


ｱﾄﾞﾚｽ
22:22:00:11:11:11
認証
サーバ
401
ｱﾄﾞﾚｽ
22:22:00:22:22:22
ファイル
サーバ
402
100
102
103
A
B
LANスイッチ
ｱﾄﾞﾚｽ
22:22:00:FF:FF:FF
C
D
E
F
104
105
106
107
情報コンセント
409
ユーザ
端末
403
ｱﾄﾞﾚｽ
22:22:FF:00:00:01

【図５】


403
ユーザ端末
100
LANスイッチ
401
認証サーバ
402
ファイルサーバ
501
ファイルサーバ宛
パケット
廃棄
502
認証サーバ宛
パケット
中継
503
ID/パスワード
要求
中継
504
ユーザID
パスワード
中継
505
状態変更
指示パケット
認証
状態変更
506
ファイルサーバ宛
パケット
中継
データ
中継

【図６】

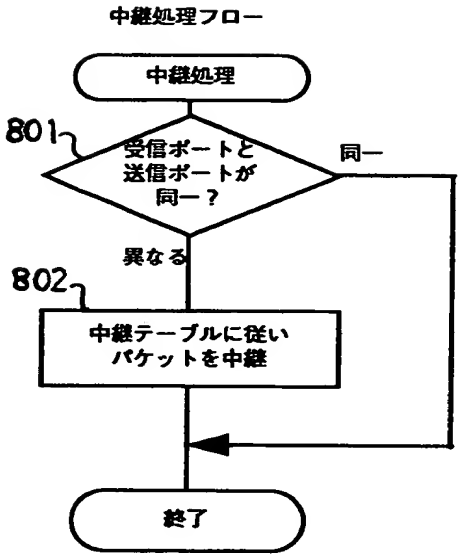

パケット受信
パケットの送信元MACアドレスが学習テーブルに未登録ならば、アドレスとしてそのアドレスと、送信ポートとしてパケットを受信したネットワークインターフェースを登録する。
601
602
宛先MACアドレスの種類
学習テーブルに未登録あるいはブロードキャストアドレス
学習テーブルに登録済み
学習テーブルの送信ポートが「X」
各ネットワークインターフェースを送信ポートとして繰り返し
学習テーブルから送信ポートを取得
603
状態指示手段に中継
605
中継処理
604
中継処理
繰り返し
終了

【図７】

108 301 302

#	アドレス	送信ポート
1	22:22:00:11:11:11	A
2	22:22:00:22:22:22	B
3	22:22:00:FF:FF:FF	X
4	22:22:FF:00:00:01	C

【図８】


中継処理フロー
中継処理
801
受信ポートと
送信ポートが
同一？
同一
異なる
802
中継テーブルに従い
パケットを中継
終了

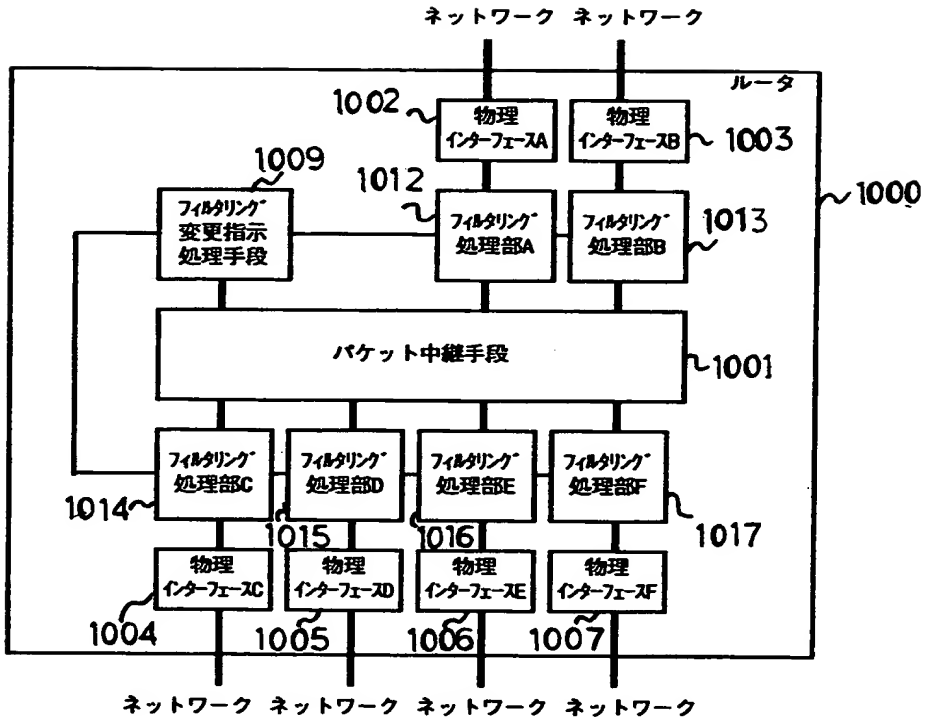
【図９】

901

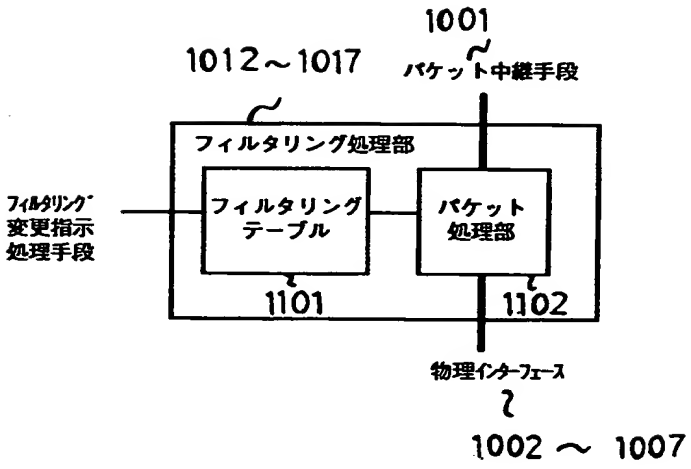
送信ポートの状態	受信ポートの状態		
	接続状態	非接続状態	状態なし
接続状態	中継	廃棄	中継
非接続状態	廃棄	廃棄	中継
状態なし	中継	中継	中継

出証特２００１－３０３２４２８

【図１０】


ネットワーク ネットワーク
ルータ
1002
物理 インターフェースA
物理 インターフェースB
1003
1009
1012
フィルタリング 変更指示 処理手段
フィルタリング 処理部A
フィルタリング 処理部B
1013
1000
パケット中継手段
1001
フィルタリング 処理部C
フィルタリング 処理部D
フィルタリング 処理部E
フィルタリング 処理部F
1014
1015
1016
1017
物理 インターフェースC
物理 インターフェースD
物理 インターフェースE
物理 インターフェースF
1004
1005
1006
1007
ネットワーク ネットワーク ネットワーク ネットワーク

【図１１】

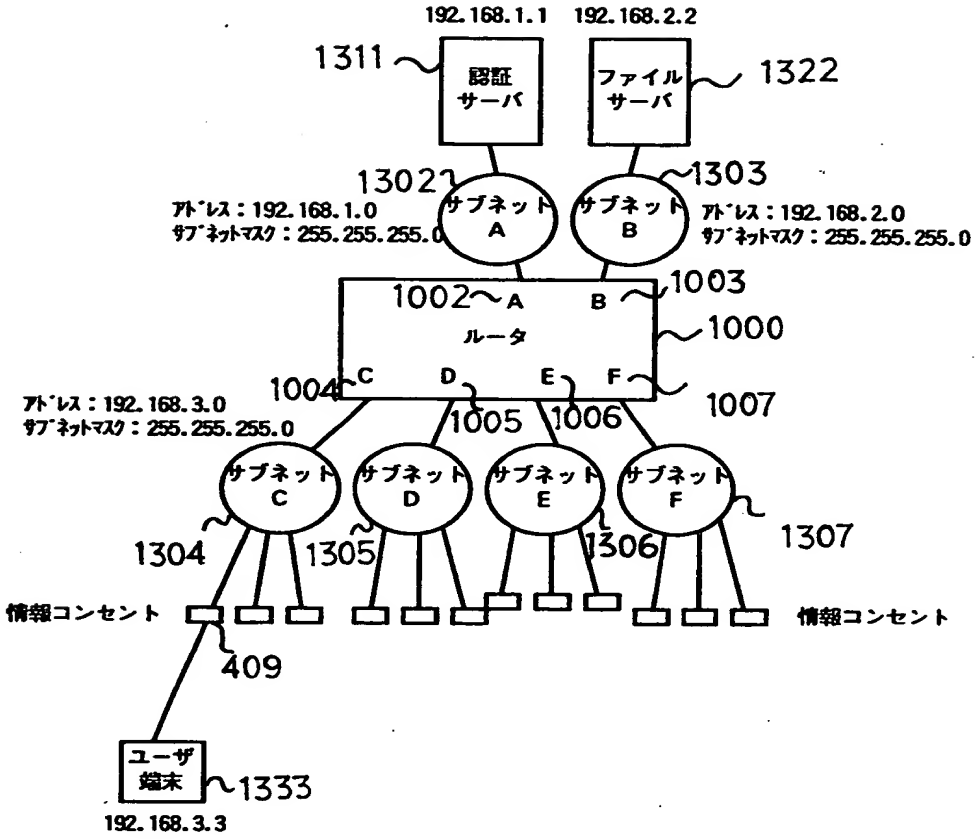

1001
1012～1017
パケット中継手段
フィルタリング処理部
フィルタリング
テーブル
パケット
処理部
フィルタリング
変更指示
処理手段
1101
1102
物理インターフェース
1002 ～ 1007

【図１２】

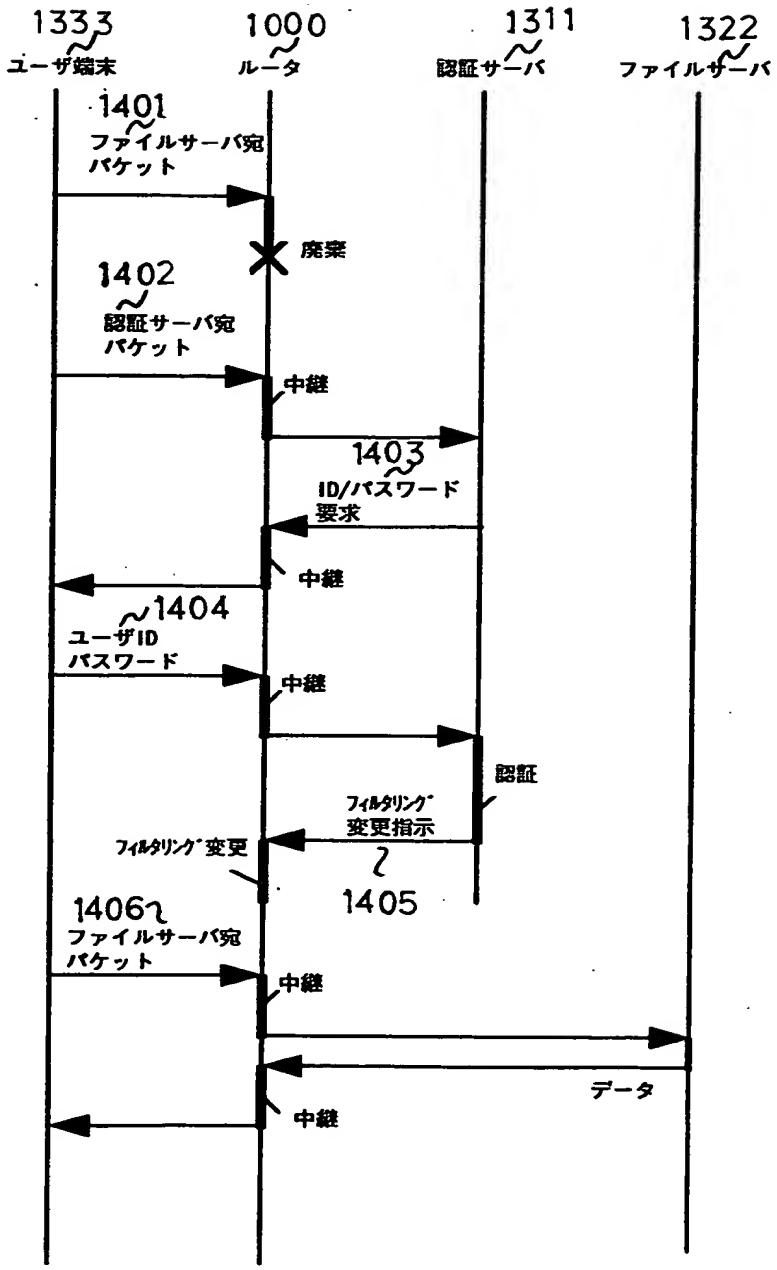
1101

#	1201 宛先アドレス条件	1202 送信元アドレス条件	1203 中継／廃棄フラグ
1	192.168.1.1	任意	中継
2	任意	任意	廃棄

【図１３】


192.168.1.1
192.168.2.2
1311
認証サーバ
ファイルサーバ
1322
1302
1303
ｱﾄﾞﾚｽ：192.168.1.0
ｻﾌﾞﾈｯﾄﾏｽｸ：255.255.255.0
サブネットA
サブネットB
ｱﾄﾞﾚｽ：192.168.2.0
ｻﾌﾞﾈｯﾄﾏｽｸ：255.255.255.0
1002
A
B
1003
ルータ
1000
C
D
E
F
1004
1005
1006
1007
ｱﾄﾞﾚｽ：192.168.3.0
ｻﾌﾞﾈｯﾄﾏｽｸ：255.255.255.0
サブネットC
サブネットD
サブネットE
サブネットF
1304
1305
1306
1307
情報コンセント
情報コンセント
409
ユーザ端末
1333
192.168.3.3

【図１４】

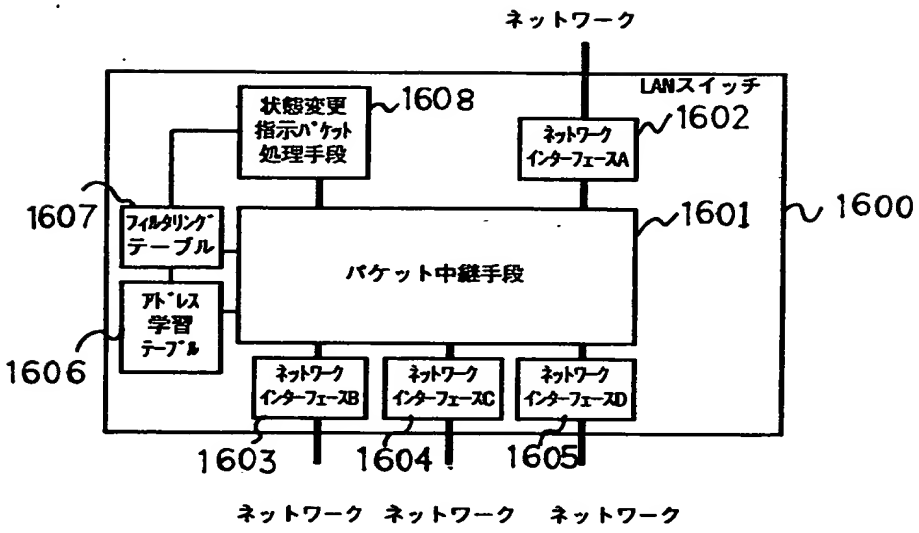

1333
ユーザ端末
1000
ルータ
1311
認証サーバ
1322
ファイルサーバ
1401
ファイルサーバ宛
パケット
廃棄
1402
認証サーバ宛
パケット
中継
1403
ID/パスワード
要求
中継
1404
ユーザID
パスワード
中継
認証
フィルタリング
変更指示
フィルタリング変更
1405
1406
ファイルサーバ宛
パケット
中継
データ
中継

【図１５】

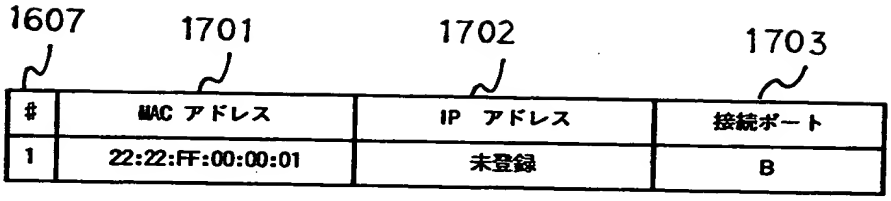
1101

#	1201 宛先アドレス条件	1202 送信元アドレス条件	1203 中継／廃棄フラグ
1	任意	192.168.3.3	中継
2	192.168.1.1	任意	中継
3	任意	任意	廃棄

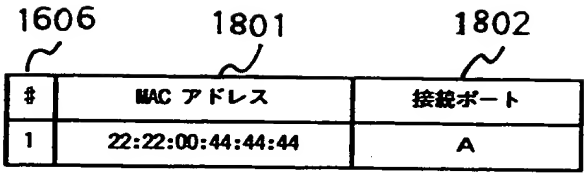
【図１６】


ネットワーク
LANスイッチ
状態変更
指示パケット
処理手段
1608
ネットワーク
インターフェースA
1602
1607
フィルタリング
テーブル
1601
1600
パケット中継手段
アドレス
学習
テーブル
1606
ネットワーク
インターフェースB
ネットワーク
インターフェースC
ネットワーク
インターフェースD
1603
1604
1605
ネットワーク
ネットワーク
ネットワーク

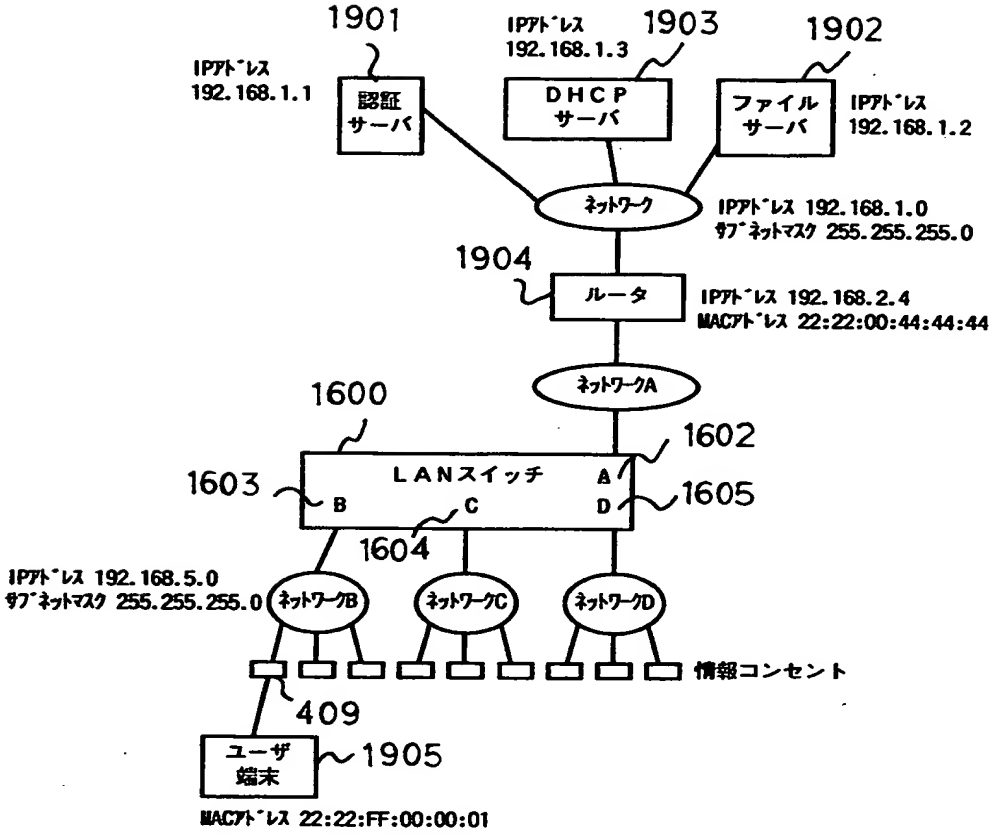
【図１７】


1607
1701
1702
1703
#
MAC アドレス
IP アドレス
接続ポート
1
22:22:FF:00:00:01
未登録
B

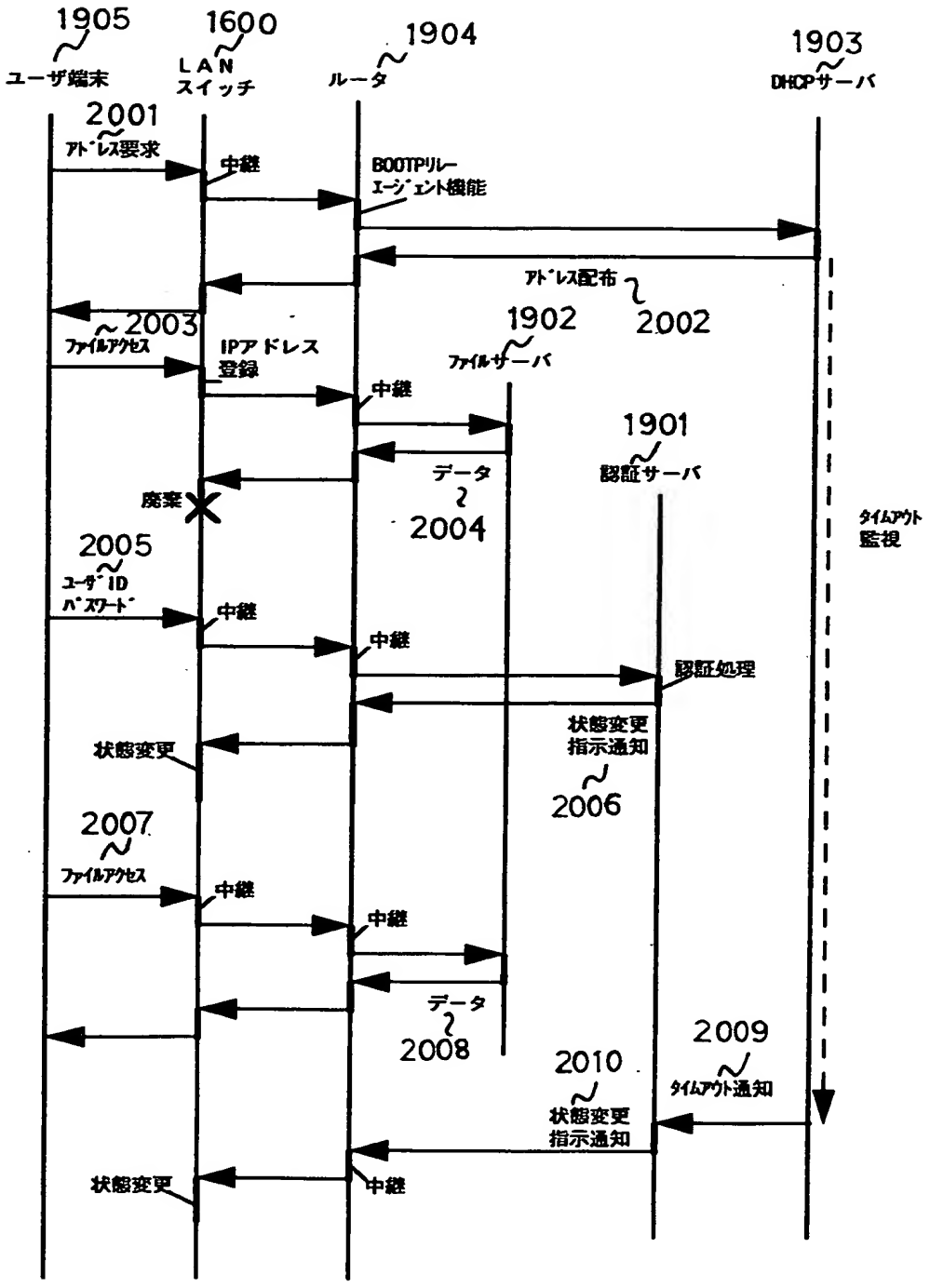
【図１８】



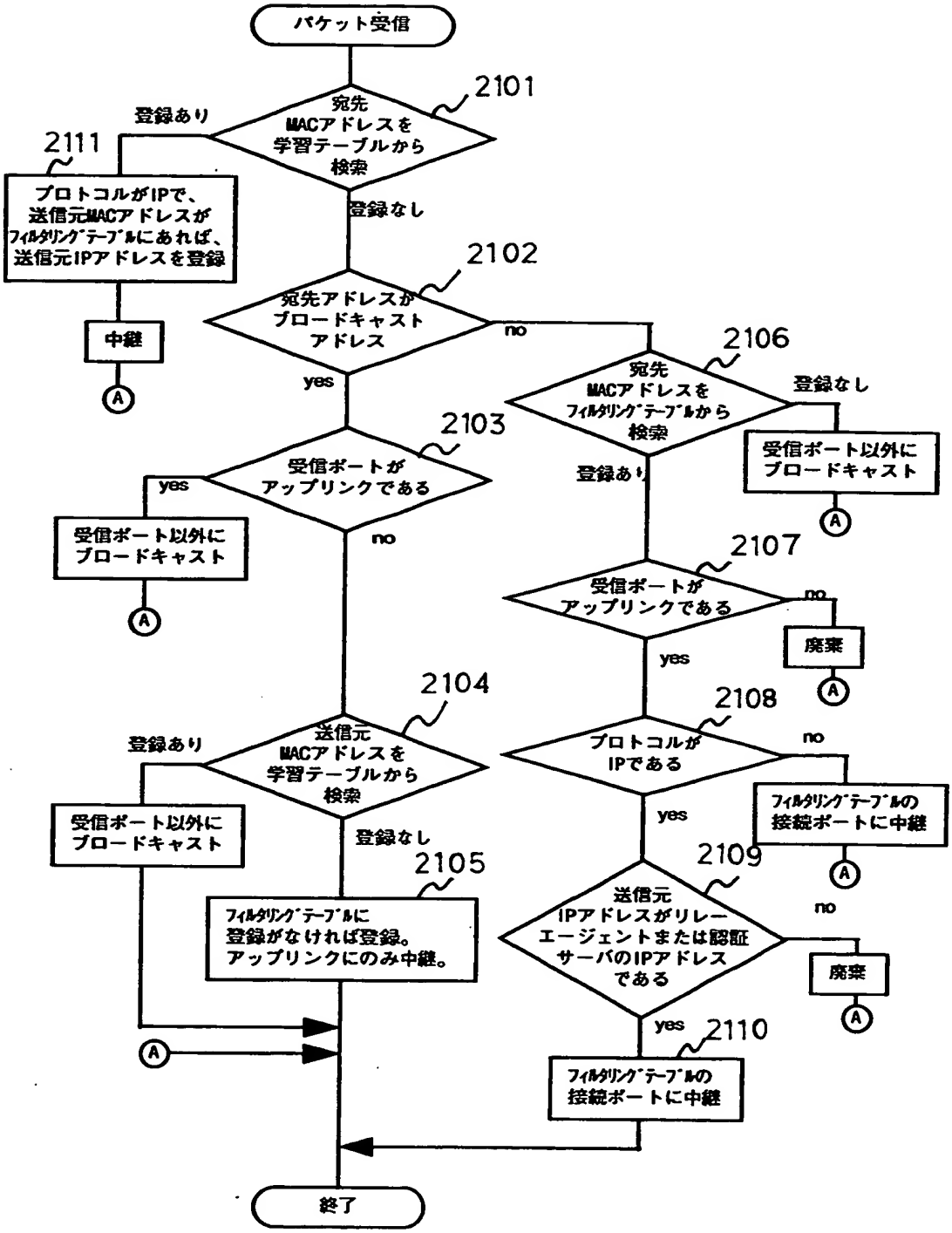
【図１９】


1901
IPアドレス
192.168.1.1
認証
サーバ
IPアドレス
192.168.1.3
1903
DHCP
サーバ
1902
ファイル
サーバ
IPアドレス
192.168.1.2
ネットワーク
IPアドレス 192.168.1.0
サブネットマスク 255.255.255.0
1904
ルータ
IPアドレス 192.168.2.4
MACアドレス 22:22:00:44:44:44
ネットワークA
1600
1602
1603
LANスイッチ
A
B
C
D
1605
1604
IPアドレス 192.168.5.0
サブネットマスク 255.255.255.0
ネットワークB
ネットワークC
ネットワークD
情報コンセント
409
ユーザ
端末
1905
MACアドレス 22:22:FF:00:00:01

【図２０】


1905
ユーザ端末
1600
LAN
スイッチ
1904
ルータ
1903
DHCPサーバ
2001
ｱﾄﾞﾚｽ要求
中継
BOOTPリレー
エージェント機能
ｱﾄﾞﾚｽ配布
2002
2003
ファイルアクセス
IPアドレス
登録
1902
ファイルサーバ
中継
1901
認証サーバ
データ
2004
廃棄
タイムアウト
監視
2005
ユーザ ID
パスワード
中継
中継
認証処理
状態変更
指示通知
2006
状態変更
2007
ファイルアクセス
中継
中継
データ
2008
2009
タイムアウト通知
2010
状態変更
指示通知
状態変更
中継

【図２１】

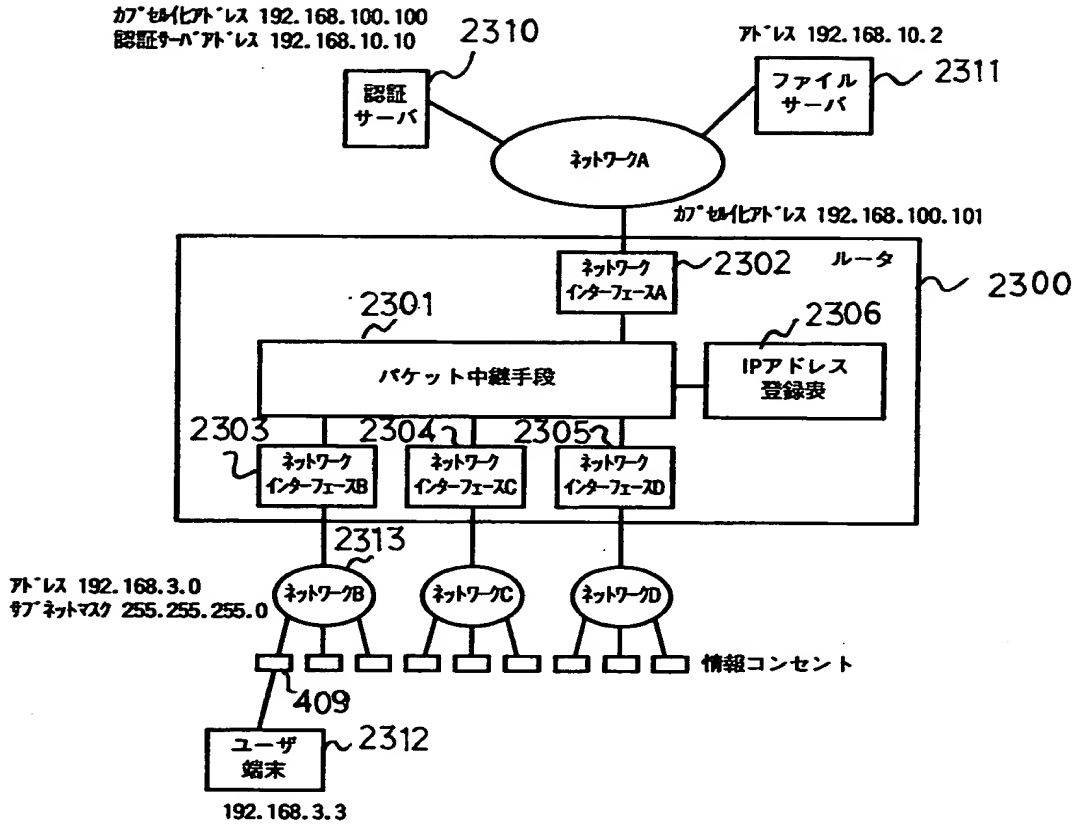

パケット受信
2101
宛先MACアドレスを学習テーブルから検索
登録あり
登録なし
2111
プロトコルがIPで、送信元MACアドレスがフィルタリングテーブルにあれば、送信元IPアドレスを登録
中継
A
2102
宛先アドレスがブロードキャストアドレス
no
yes
2103
受信ポートがアップリンクである
yes
受信ポート以外にブロードキャスト
A
no
2104
送信元MACアドレスを学習テーブルから検索
登録あり
受信ポート以外にブロードキャスト
A
登録なし
2105
フィルタリングテーブルに登録がなければ登録。アップリンクにのみ中継。
A
終了
2106
宛先MACアドレスをフィルタリングテーブルから検索
登録なし
受信ポート以外にブロードキャスト
A
登録あり
2107
受信ポートがアップリンクである
no
廃棄
A
yes
2108
プロトコルがIPである
no
フィルタリングテーブルの接続ポートに中継
A
yes
2109
送信元IPアドレスがリレーエージェントまたは認証サーバのIPアドレスである
no
廃棄
A
yes
2110
フィルタリングテーブルの接続ポートに中継

【図２２】

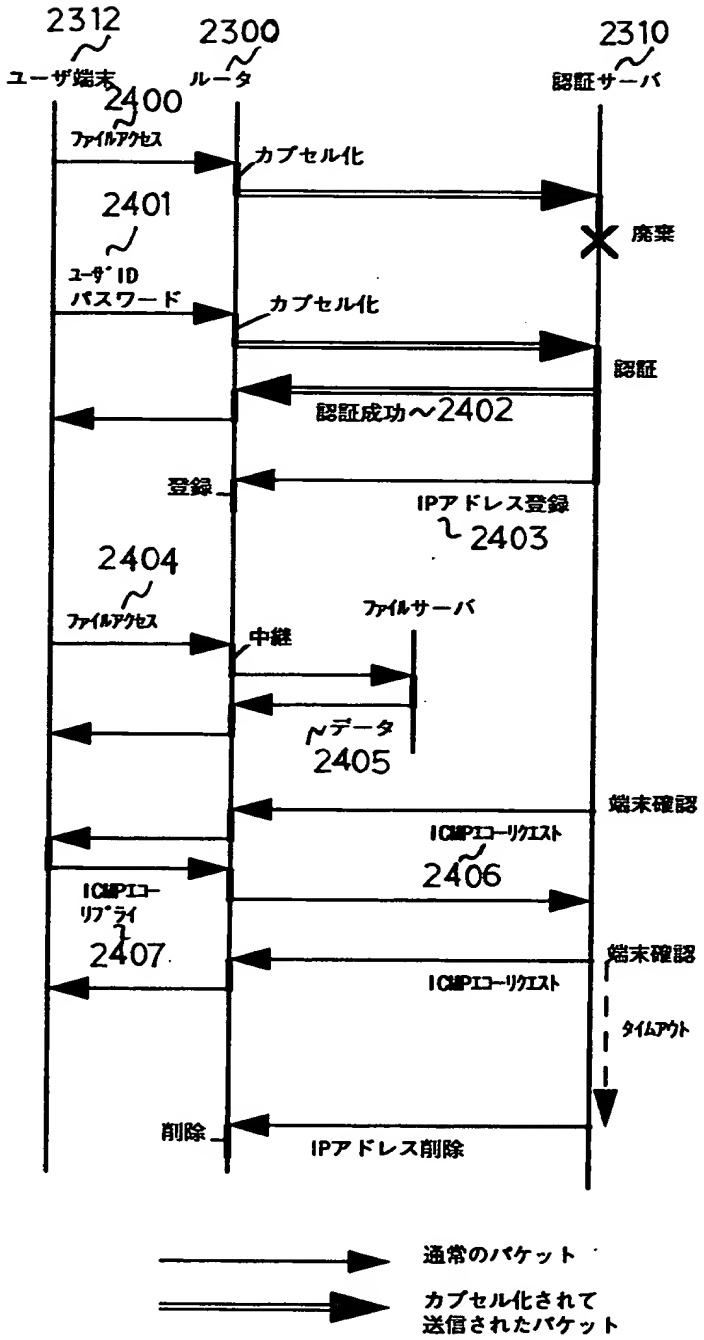
1606　1801　1802

#	MAC アドレス	接続ポート
1	22:22:00:44:44:44	A
2	22:22:FF:00:00:01	B

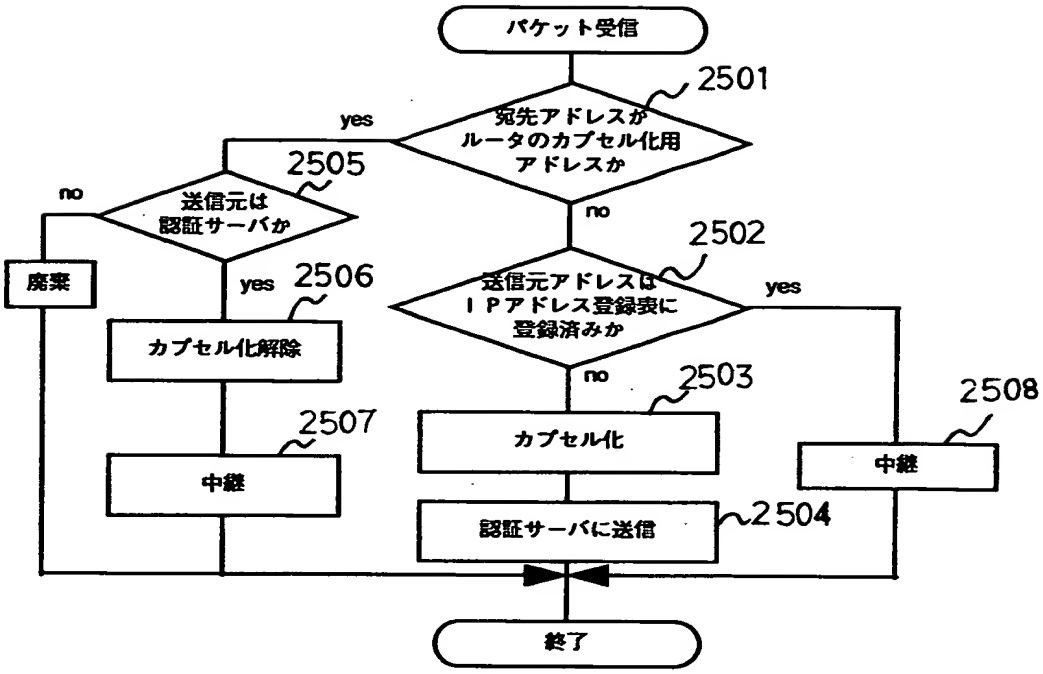
【図２３】


ｶﾌﾟｾﾙｲﾋﾞｱﾄﾞﾚｽ 192.168.100.100
認証ｻｰﾊﾞｱﾄﾞﾚｽ 192.168.10.10
2310
認証サーバ
ｱﾄﾞﾚｽ 192.168.10.2
ファイルサーバ
2311
ネットワークA
ｶﾌﾟｾﾙｲﾋﾞｱﾄﾞﾚｽ 192.168.100.101
ネットワークインターフェースA
2302
ルータ
2300
2301
2306
パケット中継手段
IPアドレス登録表
2303
2304
2305
ネットワークインターフェースB
ネットワークインターフェースC
ネットワークインターフェースD
2313
ｱﾄﾞﾚｽ 192.168.3.0
ｻﾌﾞﾈｯﾄﾏｽｸ 255.255.255.0
ネットワークB
ネットワークC
ネットワークD
情報コンセント
409
ユーザ端末
2312
192.168.3.3

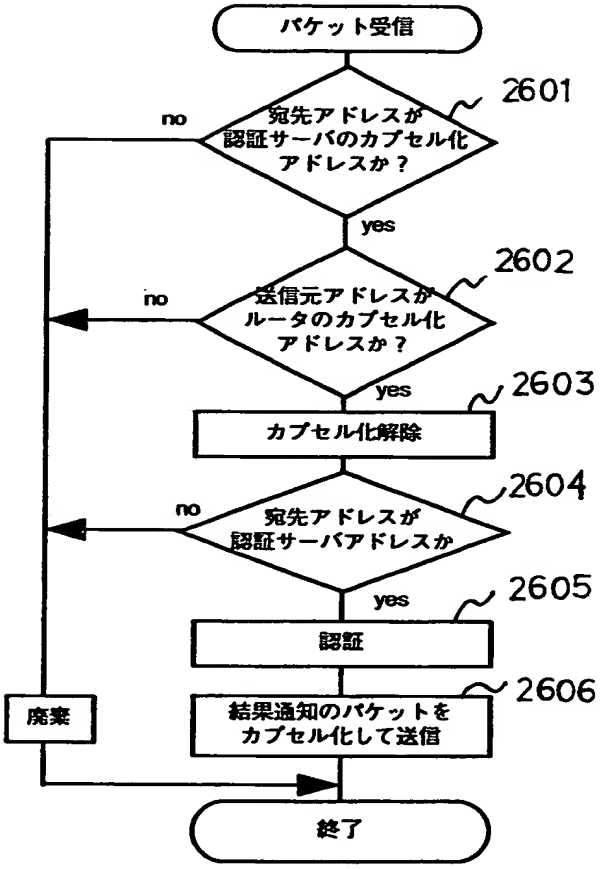
【図２４】


2312
ユーザ端末
2300
ルータ
2310
認証サーバ
2400
ファイルアクセス
カプセル化
2401
廃棄
ユーザID
パスワード
カプセル化
認証
認証成功～2402
登録
IPアドレス登録
2403
2404
ファイルアクセス
ファイルサーバ
中継
データ
2405
端末確認
ICMPエコーリクエスト
2406
ICMPエコー
リプライ
2407
端末確認
ICMPエコーリクエスト
タイムアウト
削除
IPアドレス削除
通常のパケット
カプセル化されて
送信されたパケット

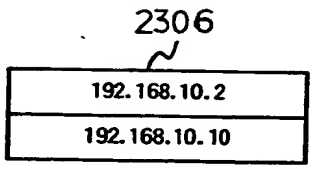
【図２５】


パケット受信
2501
宛先アドレスが
ルータのカプセル化用
アドレスか
yes
no
2505
送信元は
認証サーバか
no
yes
2502
送信元アドレスは
ＩＰアドレス登録表に
登録済みか
yes
no
廃棄
2506
カプセル化解除
2503
カプセル化
2508
中継
2507
中継
認証サーバに送信
2504
終了

【図２６】


パケット受信
2601
宛先アドレスが
認証サーバのカプセル化
アドレスか？
no
yes
2602
送信元アドレスが
ルータのカプセル化
アドレスか？
no
yes
2603
カプセル化解除
2604
宛先アドレスが
認証サーバアドレスか
no
yes
2605
認証
2606
結果通知のパケットを
カプセル化して送信
廃棄
終了

【図２７】



【書類名】　要約書

【要約】

【課題】　不正な利用者がネットワークを不正に利用することを防止する。

【解決手段】　ＬＡＮ１００は、パケット中継手段１０１、複数のネットワークインターフェース１０２～１０７、アドレス学習テーブル１０８及び状態変更指示パケット処理手段１０９を備え、状態変更指示パケット処理手段１０９は、特定のネットワークインターフェースの状態を「接続状態」、「非接続状態」及び「状態なし」のいずれかの状態に変更する指示を保持する状態変更指示パケットを、パケット中継手段１０１を介して認証サーバ４０１から受信すると共に、この状態変更指示パケットを、特定のネットワークインターフェース内の状態管理手段２０３に送信する。この状態管理手段２０３は、状態変更指示パケットに基づいて、特定のネットワークインターフェースの状態を「接続状態」、「非接続状態」及び「状態なし」のいずれかの状態に変更する。

【選択図】　図１

出証特２００１－３０３２４２８

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所